T S3/5/1

3/5/1
DIALOG(R)File 351:Derwent WPI

013608276
WPI Acc No: 2001-092484/200111
XRPX Acc No: N01-069981
Electronic storage device for guaranteeing originality of electronic data varies level of access based on if data are original data or not
Patent Assignee: RICOH KK (RICO)
Inventor: KANAI Y; YACHIDA M
Number of Countries: 002 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 10024753	A1	20001221	DE 1024753	A	20000519	200111	B
JP 2000339223	A	20001208	JP 99145340	A	19990525	200113	
JP 2001005728	A	20010112	JP 99173371	A	19990618	200118	
JP 2001147898	A	20010529	JP 99328802	A	19991118	200136	
JP 2001154577	A	20010608	JP 99338741	A	19991129	200138	
JP 2001209582	A	20010803	JP 200015092	A	20000124	200150	
JP 2001209581	A	20010803	JP 200015091	A	20000124	200150	

Priority Applications (No Type Date): JP 200015092 A 20000124; JP 99145340 A 19990525; JP 99173371 A 19990618; JP 99328802 A 19991118; JP 99338741 A 19991129; JP 200015091 A 20000124
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 10024753	A1		159	G06F-012/14	
JP 2000339223	A		29	G06F-012/14	
JP 2001005728	A		46	G06F-012/14	
JP 2001147898	A		11	G06F-015/00	
JP 2001154577	A		12	G09C-001/00	
JP 2001209582	A		18	G06F-012/14	
JP 2001209581	A		16	G06F-012/14	

Abstract (Basic): DE 10024753 A1
NOVELTY - The storage device includes a storage unit which stores electronic data consisting of a number of content files as a single original in an identifiable state. An access unit controls the access to the original electronic data at a level which is different from the level of access to non-original electronic data. The storage unit stores tamper detection information as original information corresponding to the electronic data.
DETAILED DESCRIPTION - The storage device may include a tamper detection information computing device which receives a request to re-store the electronic data as a single original using an encryption key to compute tamper detection information for each of the content files. A second tamper detection information computing device uses the encryption key to compute second temper detection information for edition management information. INDEPENDENT CLAIMS are included for an electronic storage device, an authorization verification system, an electronic storage method, an authorization verification method, damage recovery method and a storage medium for storing a program in a computer.
USE - For originality-guarantee electronic preservation systems using large-capacity storage media.
ADVANTAGE - Allows the originality of a combined document comprising multiple files to be guaranteed.

pp; 159 DwgNo 0/74
Title Terms: ELECTRONIC; STORAGE; DEVICE; GUARANTEE; ELECTRONIC; DATA; VARY ; LEVEL; ACCESS; BASED; DATA; ORIGINAL; DATA
Derwent Class: P85; T01
International Patent Class (Main): G06F-012/14; G06F-015/00
International Patent Class (Additional): G06F-003/06; G06F-009/06; G06F-012/00; G06F-012/16; G06F-017/30; G06F-017/60; G09C-001/00
File Segment: EPI; EngPI
?

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－5728
（P2001－5728A）
(43)公開日　平成13年１月12日(2001.1.12)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ 12/14	３１０Ｚ	５Ｂ０１７
	12/00	５２０	12/00	５２０Ｅ	５Ｂ０４９
		５３７		５３７Ａ	５Ｂ０７５
	17/60		15/21	Ｚ	５Ｂ０８２
	17/30		15/40	３２０Ｂ	

審査請求　未請求　請求項の数15　ＯＬ　（全 46 頁）　最終頁に続く

(21)出願番号　特願平11－173371

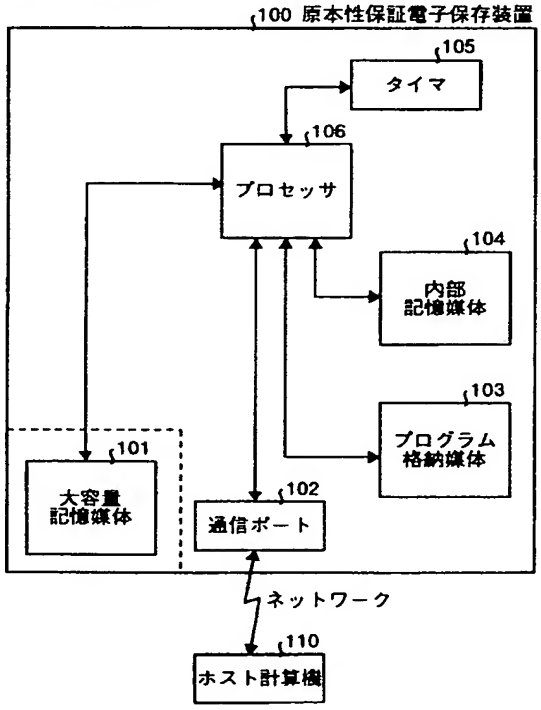
(22)出願日　平成11年６月18日(1999.6.18)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　原本性保証電子保存装置、原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　複数のファイルから形成される複合文書の原本性を効率良く保証することができる原本性保証電子保存方法および記録媒体を提供すること。
【解決手段】　複数のコンテンツファイルにより形成される電子データを一つの原本として大容量記憶媒体１０１に保存しておき、プロセッサ１０６がこの大容量記憶媒体１０１の電子データをアクセスするに際しては、原本とそうでないものとでアクセス制御のレベルを変える。



1

【特許請求の範囲】

【請求項１】　所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存装置において、

複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存する保存手段と、

前記保存工程によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうアクセス制御手段と、

を備えたことを特徴とする原本性保証電子保存装置。

【請求項２】　前記保存手段は、前記電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに前記記憶部に保存することを特徴とする請求項１に記載の原本性保証電子保存装置。

【請求項３】　前記保存手段は、前記電子データに対応する第１の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を前記属性情報とともに前記記憶部に保存することを特徴とする請求項１に記載の原本性保証電子保存装置。

【請求項４】　前記保存手段は、

前記複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定する第１の改ざん検知情報算定手段と、

前記第１の改ざん検知情報算定手段により算定された第１の改ざん検知情報を含む版管理情報を作成する版管理情報作成手段と、

前記版管理情報作成手段により作成された版管理情報に係る第２の改ざん検知情報を前記暗号鍵を用いて算定する第２の改ざん検知情報算定手段と、

前記第２の改ざん検知情報算定手段により算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を前記暗号鍵を用いて算定する第３の改ざん検知情報算定手段と、

前記第３の改ざん検知情報算定手段により算定された第３の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加手段と、

前記エントリ追加手段によりエントリが追加されたデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて算定する第４の改ざん検知情報算定手段と、

前記第４の改ざん検知情報算定手段により算定された第４の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納手段と、

を備えたことを特徴とする請求項１に記載の原本性保証電子保存装置。

【請求項５】　前記アクセス制御手段は、

外部から原本となるコンテンツファイルの読み出し要求

2

を受け付けた際に、前記記憶部から第４の改ざん検知情報および前記データリストを読み出す読み出し手段と、

前記読み出し手段により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知手段と、

前記データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、取り出したエントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知手段と、

前記記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第２の改ざん検知情報および前記復号鍵を用いて前記版管理情報の改ざん検知をおこなう第３の改ざん検知手段と、

前記版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第４の改ざん検知手段と、

前記コンテンツファイルが改ざんされていない場合に、前記記憶部に記憶したコンテンツファイルを要求元に提供する提供手段と、

を備えたことを特徴とする請求項４に記載の原本性保証電子保存装置。

【請求項６】　前記アクセス制御手段は、

外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、前記記憶部から第４の改ざん検知情報およびデータリストを読み出す読み出し手段と、

前記読み出し手段により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知手段と、

前記データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知手段と、

前記暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定する第１の改ざん検知情報算定手段と、

前記第２の改ざん検知情報算定手段により算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を前記暗号鍵を用いて算定する第３の改ざん検知情報算定手段と、

前記第３の改ざん検知情報算定手段により算定された第３の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加手段と、

前記エントリ追加手段によりエントリが追加されたデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて算定する第４の改ざん検知情報算定手段と、
前記第４の改ざん検知情報算定手段により算定された第４の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納手段と、
を備えたことを特徴とする請求項４に記載の原本性保証電子保存装置。

【請求項７】　前記アクセス制御手段は、
外部から原本となる電子データの版を指定した複製要求を受け付けた際に、前記第４の改ざん検知情報およびデータリストを読み出す読み出し手段と、
前記読み出し手段により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知手段と、前記データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知手段と、
前記属性情報から複製対象となる版に係る第２の改ざん検知情報を取り出し、該第２の改ざん検知情報および前記復号鍵を用いて版管理情報の改ざん検知をおこなう第３の改ざん検知手段と、
前記版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第４の改ざん検知手段と、
前記記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製する複製手段と、
前記複製手段により複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更する属性変更手段と、
前記属性変更手段により変更された属性コードを含む属性情報および前記暗号鍵を用いて第３の改ざん検知情報を再算定する第３の改ざん検知情報再算定手段と、
前記第３の改ざん検知情報再算定手段により算定された第３の改ざん検知情報を含むエントリにより前記データリストを更新し、更新後のデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて再算定する第４の改ざん検知情報再算定手段と、
を備えたことを特徴とする請求項４に記載の原本性保証電子保存装置。

【請求項８】　所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法において、
複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存する保存工程と、
前記保存工程によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうアクセス制御工程と、
を含んだことを特徴とする原本性保証電子保存方法。

【請求項９】　前記保存工程は、前記電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに前記記憶部に保存することを特徴とする請求項８に記載の原本性保証電子保存方法。

【請求項１０】　前記保存工程は、前記電子データに対応する第１の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を前記属性情報とともに前記記憶部に保存することを特徴とする請求項８に記載の原本性保証電子保存方法。

【請求項１１】　前記保存工程は、
前記複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定する第１の改ざん検知情報算定工程と、
前記第１の改ざん検知情報算定工程により算定された第１の改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、
前記版管理情報作成工程により作成された版管理情報に係る第２の改ざん検知情報を前記暗号鍵を用いて算定する第２の改ざん検知情報算定工程と、
前記第２の改ざん検知情報算定工程により算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を前記暗号鍵を用いて算定する第３の改ざん検知情報算定工程と、
前記第３の改ざん検知情報算定工程により算定された第３の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加工程と、
前記エントリ追加工程によりエントリが追加されたデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて算定する第４の改ざん検知情報算定工程と、前記第４の改ざん検知情報算定工程により算定された第４の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納工程と、
を含んだことを特徴とする請求項８に記載の原本性保証電子保存方法。

【請求項１２】　前記アクセス制御工程は、
外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、前記記憶部から第４の改ざん検知情報および前記データリストを読み出す読み出し工程と、
前記読み出し工程により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知工程と、

5

前記データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、取り出したエントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知工程と、

前記記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第２の改ざん検知情報および前記復号鍵を用いて前記版管理情報の改ざん検知をおこなう第３の改ざん検知工程と、

前記版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第４の改ざん検知工程と、

前記コンテンツファイルが改ざんされていない場合に、前記記憶部に記憶したコンテンツファイルを要求元に提供する提供工程と、

を含んだことを特徴とする請求項１１に記載の原本性保証電子保存方法。

【請求項１３】　前記アクセス制御工程は、

外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、前記記憶部から第４の改ざん検知情報およびデータリストを読み出す読み出し工程と、

前記読み出し工程により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知工程と、

前記データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知工程と、

前記暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定する第１の改ざん検知情報算定工程と、

前記第２の改ざん検知情報算定工程により算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を前記暗号鍵を用いて算定する第３の改ざん検知情報算定工程と、

前記第３の改ざん検知情報算定工程により算定された第３の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加工程と、

前記エントリ追加工程によりエントリが追加されたデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて算定する第４の改ざん検知情報算定工程と、

前記第４の改ざん検知情報算定工程により算定された第４の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納工程と、

6

を含んだことを特徴とする請求項１１に記載の原本性保証電子保存方法。

【請求項１４】　前記アクセス制御工程は、

外部から原本となる電子データの版を指定した複製要求を受け付けた際に、前記第４の改ざん検知情報およびデータリストを読み出す読み出し工程と、

前記読み出し工程により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知工程と、前記データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知工程と、

前記属性情報から複製対象となる版に係る第２の改ざん検知情報を取り出し、該第２の改ざん検知情報および前記復号鍵を用いて版管理情報の改ざん検知をおこなう第３の改ざん検知工程と、

前記版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第４の改ざん検知工程と、

前記記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製する複製工程と、

前記複製工程により複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更する属性変更工程と、

前記属性変更工程により変更された属性コードを含む属性情報および前記暗号鍵を用いて第３の改ざん検知情報を再算定する第３の改ざん検知情報再算定工程と、

前記第３の改ざん検知情報再算定工程により算定された第３の改ざん検知情報を含むエントリにより前記データリストを更新し、更新後のデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて再算定する第４の改ざん検知情報再算定工程と、

を含んだことを特徴とする請求項１１に記載の原本性保証電子保存方法。

【請求項１５】　前記請求項８～１４のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存装置、原本性保証電子保存方法および記録媒体に関し、特に、複数のファイルから形成される複合文書の原本性を効率良く保証することができる原本性保証電子保存装置、原本性保証電子保存方法および記録媒体に関す

る。

【０００２】

【従来の技術】近年のコンピュータ技術の進展に伴うペーパーレス化の進展に伴って、紙によって原本書類として保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。

【０００３】たとえば、「金井他：原本性保証電子保存システムの開発－システムの構築－，Medical Imaging Tecnology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発，（特）情報処理振興事業協会発行　創造的ソフトウエア育成事業およびエレクトロニック・コマース推進事業　最終成果発表会論文集　創造的ソフトウエア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。

【０００４】かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、これらの従来技術のものは、原本となる電子文書が１つのファイルで形成されることを前提としており、ＨＴＭＬ、ＸＭＬおよびＳＧＭＬのように複数のファイルによって電子文書が形成される場合を考慮したものではないので、かかる複数のファイルによって形成される電子文書（以下「複合文書」と言う）の原本性を効率良く保証することができないという問題がある。

【０００６】すなわち、従来技術を用いてかかる複合文書の原本性を保証するには、複数のファイルを一つのファイルにまとめた後に原本性保証電子保存装置に保存するか、または各ファイルをそれぞれ別個の原本として原本性保証電子保存装置に保存せざる得ない。

【０００７】しかし、複数のファイルを一つのファイルにまとめることとしたのでは、どこからどこまでがどのファイルに相当するデータであるかを外部アプリケーションプログラムなどによって管理しなければならないため、その管理負担が大きいという問題がある。また、一つの塊にまとめられたデータは特殊なフォーマットとなってしまうために、外部アプリケーションとして取り扱い難くなり、原本データの見読性が低下するという問題もある。

【０００８】一方、各ファイルをそれぞれ別個の原本として保存することとしたのでは、各原本がもともと一つの文書を形成するにもかかわらず、各原本がそれぞれ別個に編集され、次第に各原本の相互関係が不明確になるおそれがある。

【０００９】これらのことから、複数のファイルから形

成される複合文書の原本性を原本性保証電子保存装置においていかに効率良く保証するかが極めて重要な課題となっている。

【００１０】この発明は、上記問題（課題）に鑑みてなされたものであり、複数のファイルから形成される複合文書の原本性を効率良く保証することができる原本性保証電子保存装置、原本性保証電子保存方法および記録媒体を提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成するために、請求項１の発明に係る原本性保証電子保存装置は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法において、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存する保存手段と、前記保存手段によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうアクセス制御手段と、を備えたことを特徴とする。

【００１２】この請求項１の発明によれば、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうこととしたので、複数のファイルから形成される複合文書の原本性を効率良く保証することができる。

【００１３】また、請求項２の発明に係る原本性保証電子保存装置は、前記保存手段は、前記電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに前記記憶部に保存することを特徴とする。

【００１４】この請求項２の発明によれば、電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに記憶部に保存することとしたので、効率良く改ざん検知をおこなうことができる。

【００１５】また、請求項３の発明に係る原本性保証電子保存装置は、前記保存手段は、前記電子データに対応する第１の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を前記属性情報とともに前記記憶部に保存することを特徴とする。

【００１６】この請求項３の発明によれば、電子データに対応する第１の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を属性情報とともに記憶部に保存することとしたので、電子データ並びにアクセス履歴を含む改ざんを効率良く検知することができる。

【００１７】また、請求項４の発明に係る原本性保証電

子保存装置は、前記保存手段は、前記複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定する第１の改ざん検知情報算定手段と、前記第１の改ざん検知情報算定手段により算定された第１の改ざん検知情報を含む版管理情報を作成する版管理情報作成手段と、前記版管理情報作成手段により作成された版管理情報に係る第２の改ざん検知情報を前記暗号鍵を用いて算定する第２の改ざん検知情報算定手段と、前記第２の改ざん検知情報算定手段により算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を前記暗号鍵を用いて算定する第３の改ざん検知情報算定手段と、前記第３の改ざん検知情報算定手段により算定された第３の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加手段と、前記エントリ追加手段によりエントリが追加されたデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて算定する第４の改ざん検知情報算定手段と、前記第４の改ざん検知情報算定手段により算定された第４の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納手段と、を備えたことを特徴とする。

【００１８】この請求項４の発明によれば、複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定し、算定した第１の改ざん検知情報を含む版管理情報を作成して第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を算定し、算定した第３の改ざん検知情報を含むデータエントリを作成して記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第４の改ざん検知情報を算定し、算定した第４の改ざん検知情報と複数のコンテンツとを記憶部に格納することとしたので、複数のコンテンツファイルからなる新規データを改ざん防止措置を施しつつ効率良く格納することができる。

【００１９】また、請求項５の発明に係る原本性保証電子保存装置は、前記アクセス制御手段は、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、前記記憶部から第４の改ざん検知情報および前記データリストを読み出す読み出し手段と、前記読み出し手段により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知手段と、前記データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、取り出したエントリ

に含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知手段と、前記記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第２の改ざん検知情報および前記復号鍵を用いて前記版管理情報の改ざん検知をおこなう第３の改ざん検知手段と、前記版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第４の改ざん検知手段と、前記コンテンツファイルが改ざんされていない場合に、前記記憶部に記憶したコンテンツファイルを要求元に提供する提供手段と、を備えたことを特徴とする。

【００２０】この請求項５の発明によれば、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、記憶部から第４の改ざん検知情報およびデータリストを読み出し、読み出した第４の改ざん検知情報および復号鍵を用いてデータリストの改ざん検知をおこない、データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、このエントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第２の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および復号鍵を用いてコンテンツファイルの改ざん検知をおこない、コンテンツファイルが改ざんされていない場合に、記憶部に記憶したコンテンツファイルを要求元に提供することとしたので、多段階に渡って改ざんを防止しつつコンテンツファイルの読み出しを効率良くおこなうことができる。

【００２１】また、請求項６の発明に係る原本性保証電子保存装置は、前記アクセス制御手段は、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、前記記憶部から第４の改ざん検知情報およびデータリストを読み出す読み出し手段と、前記読み出し手段により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知手段と、前記データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知手段と、前記暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定する第１の改ざん検知情報算定手段と、前記第２の改ざん検知情報算定手

段により算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を前記暗号鍵を用いて算定する第３の改ざん検知情報算定手段と、前記第３の改ざん検知情報算定手段により算定された第３の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加手段と、前記エントリ追加手段によりエントリが追加されたデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて算定する第４の改ざん検知情報算定手段と、前記第４の改ざん検知情報算定手段により算定された第４の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納手段と、を備えたことを特徴とする。

【００２２】この請求項６の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、記憶部から第４の改ざん検知情報およびデータリストを読み出し、読み出した第４の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定し、算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を暗号鍵を用いて算定し、算定された第３の改ざん検知情報を含むデータエントリを作成し、記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第４の改ざん検知情報を算定し、算定された第４の改ざん検知情報と複数のコンテンツとを記憶部に格納することとしたので、電子データが複数のコンテンツファイルからなる場合であっても、バージョンアップを効率良くおこなうことができる。

【００２３】また、請求項７の発明に係る原本性保証電子保存装置は、前記アクセス制御手段は、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、前記第４の改ざん検知情報およびデータリストを読み出す読み出し手段と、前記読み出し手段により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知手段と、前記データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知手段と、前記属性情報から複製対象となる版に係る第２の改ざん検知情報を取り出し、該第２の改ざん検知情報および前記復号鍵を用いて版管理情報の改ざん検知をおこなう第３の改ざん検知手段と、前記版管

理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第４の改ざん検知手段と、前記記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製する複製手段と、前記複製手段により複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更する属性変更手段と、前記属性変更手段により変更された属性コードを含む属性情報および前記暗号鍵を用いて第３の改ざん検知情報を再算定する第３の改ざん検知情報再算定手段と、前記第３の改ざん検知情報再算定手段により算定された第３の改ざん検知情報を含むエントリにより前記データリストを更新し、更新後のデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて再算定する第４の改ざん検知情報再算定手段と、を備えたことを特徴とする。

【００２４】この請求項７の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、第４の改ざん検知情報およびデータリストを読み出し、読み出した第４の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、属性情報から複製対象となる版に係る第２の改ざん検知情報を取り出し、該第２の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および復号鍵を用いて前記コンテンツファイルの改ざん検知をおこない、記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製し、複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更し、変更された属性コードを含む属性情報および暗号鍵を用いて第３の改ざん検知情報を再算定し、再算定された第３の改ざん検知情報を含むエントリによりデータリストを更新し、更新後のデータリストに係る第４の改ざん検知情報を暗号鍵を用いて再算定することとしたので、電子データが複数のコンテンツファイルからなる場合であっても、版を指定した複製を効率良くおこなうことができる。

【００２５】また、請求項８の発明に係る原本性保証電子保存方法は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法において、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存する保存工程と、前記保存工程によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベ

ルのアクセス制御をおこなうアクセス制御工程と、を含んだことを特徴とする。

【００２６】この請求項８の発明によれば、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうこととしたので、複数のファイルから形成される複合文書の原本性を効率良く保証することができる。

【００２７】また、請求項９の発明に係る原本性保証電子保存方法は、前記保存工程は、前記電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに前記記憶部に保存することを特徴とする。

【００２８】この請求項９の発明によれば、電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに記憶部に保存することとしたので、効率良く改ざん検知をおこなうことができる。

【００２９】また、請求項１０の発明に係る原本性保証電子保存方法は、前記保存工程は、前記電子データに対応する第１の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を前記属性情報とともに前記記憶部に保存することを特徴とする。

【００３０】この請求項１０の発明によれば、電子データに対応する第１の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を属性情報とともに記憶部に保存することとしたので、電子データ並びにアクセス履歴を含む改ざんを効率良く検知することができる。

【００３１】また、請求項１１の発明に係る原本性保証電子保存方法は、前記保存工程は、前記複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定する第１の改ざん検知情報算定工程と、前記第１の改ざん検知情報算定工程により算定された第１の改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、前記版管理情報作成工程により作成された版管理情報に係る第２の改ざん検知情報を前記暗号鍵を用いて算定する第２の改ざん検知情報算定工程と、前記第２の改ざん検知情報算定工程により算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を前記暗号鍵を用いて算定する第３の改ざん検知情報算定工程と、前記第３の改ざん検知情報算定工程により算定された第３の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加

工程と、前記エントリ追加工程によりエントリが追加されたデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて算定する第４の改ざん検知情報算定工程と、前記第４の改ざん検知情報算定工程により算定された第４の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納工程と、を含んだことを特徴とする。

【００３２】この請求項１１の発明によれば、複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定し、算定した第１の改ざん検知情報を含む版管理情報を作成して第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を算定し、算定した第３の改ざん検知情報を含むデータエントリを作成して記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第４の改ざん検知情報を算定し、算定した第４の改ざん検知情報と複数のコンテンツとを記憶部に格納することとしたので、複数のコンテンツファイルからなる新規データを改ざん防止措置を施しつつ効率良く格納することができる。

【００３３】また、請求項１２の発明に係る原本性保証電子保存方法は、前記アクセス制御工程は、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、前記記憶部から第４の改ざん検知情報および前記データリストを読み出す読み出し工程と、前記読み出し工程により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知工程と、前記データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、取り出したエントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知工程と、前記記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第２の改ざん検知情報および前記復号鍵を用いて前記版管理情報の改ざん検知をおこなう第３の改ざん検知工程と、前記版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第４の改ざん検知工程と、前記コンテンツファイルが改ざんされていない場合に、前記記憶部に記憶したコンテンツファイルを要求元に提供する提供工程と、を含んだことを特徴とする。

【００３４】この請求項１２の発明によれば、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、記憶部から第４の改ざん検知情報およびデー

15

タリストを読み出し、読み出した第４の改ざん検知情報および復号鍵を用いてデータリストの改ざん検知をおこない、データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、このエントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第２の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および復号鍵を用いてコンテンツファイルの改ざん検知をおこない、コンテンツファイルが改ざんされていない場合に、記憶部に記憶したコンテンツファイルを要求元に提供することとしたので、多段階に渡って改ざんを防止しつつコンテンツファイルの読み出しを効率良くおこなうことができる。

【００３５】また、請求項１３の発明に係る原本性保証電子保存方法は、前記アクセス制御工程は、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、前記記憶部から第４の改ざん検知情報およびデータリストを読み出す読み出し工程と、前記読み出し工程により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知工程と、前記データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知工程と、前記暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定する第１の改ざん検知情報算定工程と、前記第２の改ざん検知情報算定工程により算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を前記暗号鍵を用いて算定する第３の改ざん検知情報算定工程と、前記第３の改ざん検知情報算定工程により算定された第３の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加工程と、前記エントリ追加工程によりエントリが追加されたデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて算定する第４の改ざん検知情報算定工程と、前記第４の改ざん検知情報算定工程により算定された第４の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納工程と、を含んだことを特徴とする。

【００３６】この請求項１３の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、記憶部から第４の改ざん検知情報およびデータリス

16

トを読み出し、読み出した第４の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定し、算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を暗号鍵を用いて算定し、算定された第３の改ざん検知情報を含むデータエントリを作成し、記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第４の改ざん検知情報を算定し、算定された第４の改ざん検知情報と複数のコンテンツとを記憶部に格納することとしたので、電子データが複数のコンテンツファイルからなる場合であっても、バージョンアップを効率良くおこなうことができる。

【００３７】また、請求項１４の発明に係る原本性保証電子保存方法は、前記アクセス制御工程は、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、前記第４の改ざん検知情報およびデータリストを読み出す読み出し工程と、前記読み出し工程により読み出された第４の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第１の改ざん検知工程と、前記データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第２の改ざん検知工程と、前記属性情報から複製対象となる版に係る第２の改ざん検知情報を取り出し、該第２の改ざん検知情報および前記復号鍵を用いて版管理情報の改ざん検知をおこなう第３の改ざん検知工程と、前記版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第４の改ざん検知工程と、前記記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製する複製工程と、前記複製工程により複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更する属性変更工程と、前記属性変更工程により変更された属性コードを含む属性情報および前記暗号鍵を用いて第３の改ざん検知情報を再算定する第３の改ざん検知情報再算定工程と、前記第３の改ざん検知情報再算定工程により算定された第３の改ざん検知情報を含むエントリにより前記データリストを更新し、更新後のデータリストに係る第４の改ざん検知情報を前記暗号鍵を用いて再算定する第４の改ざん検知情報再算定工程と、を含んだことを特徴とする。

【００３８】この請求項１４の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、第４の改ざん検知情報およびデータリストを読み出し、読み出した第４の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、属性情報から複製対象となる版に係る第２の改ざん検知情報を取り出し、該第２の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および復号鍵を用いて前記コンテンツファイルの改ざん検知をおこない、記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製し、複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更し、変更された属性コードを含む属性情報および暗号鍵を用いて第３の改ざん検知情報を再算定し、再算定された第３の改ざん検知情報を含むエントリによりデータリストを更新し、更新後のデータリストに係る第４の改ざん検知情報を暗号鍵を用いて再算定することとしたので、電子データが複数のコンテンツファイルからなる場合であっても、版を指定した複製を効率良くおこなうことができる。

【００３９】また、請求項１５の発明に係る記録媒体は、前記請求項８～１４のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項８～１４の動作をコンピュータによって実現することができる。

【００４０】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【００４１】図１は、本実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。同図に示すように、この原本性保証電子保存装置１００は、原本となる電子データを記憶し、ネットワークを介してホスト計算機１１０からアクセスされる装置であり、大容量記憶媒体１０１と、通信ポート１０２と、プログラム格納媒体１０３と、内部記憶媒体１０４と、タイマ１０５と、プロセッサ１０６とからなる。

【００４２】大容量記憶媒体１０１は、原本となる電子データなどを記憶する大容量の二次記憶装置であり、たとえば光磁気ディスクやＣＤ－Ｒなどからなる。通信ポート１０２は、ネットワークを介したホスト計算機との

通信をおこなうためのインターフェース部であり、たとえばＬＡＮカードなどの通信モデムなどからなる。

【００４３】プログラム格納媒体１０３は、主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを格納したメモリであり、たとえば書換可能なＥＥＰＲＯＭや読み出し専用のＲＯＭなどからなる。

【００４４】内部記憶媒体１０４は、各種プログラムの実行に必要となるパラメータを記憶するＥＥＰＲＯＭなどからなるメモリであり、具体的には、装置暗号鍵、装置復号鍵、媒体認証コードリスト、最新データ識別番号、タイマ設定履歴ファイルおよびアカウント管理リストなどを記憶する。タイマ１０５は、プロセッサ１０６がプログラムの実行時に所得する時刻を計時するタイマである。

【００４５】なお、大容量記憶媒体１０１については、図中に破線で示したように原本性保証電子保存装置１００から取り外し可能としても良いが、その他の構成部位については原本性保証電子保存装置１００と物理的に一体化し、通信ポート１０２以外からのアクセスを受け付けない耐タンパー性を有する構成にする。

【００４６】ただし、この耐タンパー性には、筐体を開けられないようにシールを貼る程度のレベルから、筐体を開けた場合に装置が動作しなくなるレベルまで様々なものがあるが、本発明はこの耐タンパー性のレベルには特段の制限を受けない。

【００４７】プロセッサ１０６は、プログラム格納媒体１０３に格納された主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを読み出して実行する制御装置である。

【００４８】具体的には、このプロセッサ１０６は、ユーザから保存要求のあったデータを大容量記憶媒体１０１に保存する際に、あとでデータの改ざんを検出できるようにするために、内部記憶媒体１０４に記憶したプライベートキーを用いて保存するデータにメッセージ認証子（ＭＡＣ：Message Authentication Code）を付加する。なお、このメッセージ認証子は、たとえば公開鍵暗号方式を採用した場合には、ディジタル署名として付加するデータに該当する。

【００４９】また、データそのものの不正な抹消を検出するために、大容量記憶媒体１０１に記憶されているデータのリストに対してもメッセージ認証子を付加し、さらにたとえば大容量記憶媒体１０１の状態を過去の状態に戻すような不正なすり替えを検出するために、大容量記憶媒体１０１の媒体識別番号と、その媒体のデータリストに対するメッセージ認証子の対を内部記憶媒体１０４に記憶して管理する。

【００５０】また、データ作成日などを不正に変更することができないように、タイマ１０５から現在時刻を取

得し、この時刻をデータの属性として付与するとともに、原本性保証電子保存装置１００内部でオリジナルな電子データである原本データとそのコピーとを区別することができるように、「仮原本」、「原本」および「謄本」といった属性をデータに付与して管理する。たとえば、「原本」という属性が付与されたデータをコピーした場合には、このコピーしたデータに「謄本」という属性が付与される。

【００５１】なお、この属性は外部から変更することはできず、また大容量記憶媒体１０１を取り外して外部にてその属性を改ざんしたとしても、この大容量記憶媒体１０１を装置に装着した際に改ざんの有無を検出する。

【００５２】次に、図１に示した大容量記憶媒体１０１に保存する保存データのデータ構造について説明する。図２は、図１に示した大容量記憶媒体１０１に保存する保存データのデータ構造の一例を示す説明図である。同図に示すように、この保存データ２００は、バージョン１に係るデータ２１０と、バージョン２に係るデータ２２０と、バージョン３に係るデータ２３０とからなる。

【００５３】そして、このバージョン１の段階では、コンテンツ１～３という３つのコンテンツを有しているが、バージョン２になる際にコンテンツ４が付加され、さらにバージョン３になる際に３番目のコンテンツ３が削除されている。

【００５４】このように、かかる大容量記憶媒体１０１に保存する保存データは、複数のコンテンツからなるデータを各バージョンごとに保存している。なお、図中に破線で示すコンテンツは、コンテンツ属性情報のみが存在するものであり、コンテンツデータファイルそのものは前バージョンのコンテンツデータファイルを参照するよう構成している。

【００５５】次に、図１に示した大容量記憶媒体１０１に保存する保存データの配置について説明する。保存データは、データ識別番号（たとえば「R01093-00123210」）をフォルダ名とするフォルダの下に、該データ識別番号をファイル名とするデータ属性情報ファイル（たとえば「R01093-00123210.dat」）を格納し、バージョンごとにバージョン番号をフォルダ名とするフォルダ（たとえば「ver.1」）を作成して、そのフォルダ内にコンテンツのデータファイルとバージョン属性情報ファイルとを格納する。

【００５６】バージョン属性情報ファイルは、ファイル名としてデータ識別番号の後ろにバージョン番号をつけたもの（たとえば「R01093-00123210-1.dat」）とし、謄本データについては、謄本データであることが直ちに判明するようにデータ識別番号の先頭に「C-」を含める。

【００５７】また、原本性保証電子保存装置１００が独自に管理するファイル、たとえば媒体識別番号ファイルおよび保存データリストファイルは、保存データとは別のフォルダ（system）に格納する。

【００５８】

具体的には、

```
/documents
    /R01093-00123210                    ；データごとのフォルダ
        R01093-00123210.dat             ；データ属性情報ファイル
        /ver.1                          ；バージョンごとのフォルダ
            R01093-00123210-1.dat       ；バージョン属性情報ファイル
            index.htm                   ；コンテンツデータ＃１
            icon.gif                     ；コンテンツデータ＃２
            context.htm                  ；コンテンツデータ＃３
        /ver.2
            R01093-00123210-2.dat
            context.htm
    /R01093-00123211
        R01093-00123211.dat
        /ver.1
            R01093-00123211-1.dat
            main.xml
            theme.dtd
            theme.xsl
    /C-R03055-00000107
        C-R03055-00000107.dat
        /ver.5
            C-R03055-00000107-5.dat
            frontpaper.doc
```

21

```
                toc.doc
                chapter1.doc
                chapter2.doc
                appendix.doc
            /...
        /system
            medium.id
            R01093-0012.list
```

のように保存データの配置を記述する。

【００５９】次に、図１に示した原本性保証電子保存装置１００による新規データの保存処理について図３～図８を用いて説明する。図３は、図１に示した原本性保証電子保存装置１００による新規データの保存処理手順を示すフローチャートである。

【００６０】図３に示すように、原本性保証電子保存装置１００は、まず最初に大容量記憶媒体１０１がマウントされているか否かを判定し（ステップＳ３０１）、大容量記憶媒体１０１がマウントされていない場合には（ステップＳ３０１肯定）、エラー処理をおこなった後に（ステップＳ３０２）、処理を終了する。

【００６１】これに対して、大容量記憶媒体１０１がマウントされている場合には（ステップＳ３０１否定）、通信ポート１０２を介して外部からデータ属性コード、コンテンツ数、コンテンツ名およびコンテンツデータを受け取る（ステップＳ３０３）。そして、受け取ったデータ属性コードが「原本」、「仮原本」または「一般」のいずれでかに該当するか否かを確認し（ステップＳ３０４）、いずれににも該当しない場合には（ステップＳ３０５肯定）、エラー処理をおこなった後に（ステップＳ３０２）、処理を終了する。

【００６２】これに対して、このデータ属性コードが「原本」、「仮原本」または「一般」のいずれかであれば（ステップＳ３０４否定）、データ属性コードが「一般」であるか否かをさらに判断し（ステップＳ３０５）、「一般」である場合には（ステップＳ３０５肯定）、受け取ったデータを受け取ったデータ名で大容量記憶媒体１０１に保存して処理を終了する（ステップＳ３０６）。

【００６３】一方、このデータ属性コードが「一般」でない場合には（ステップＳ３０５否定）、初版としてバージョン属性情報の作成処理をおこなった後に（ステップＳ３０７）、データ属性情報を作成処理する（ステップＳ３０８）。

【００６４】その後、受け取ったコンテンツデータをすべてデータファイルとして大容量記憶媒体１０１に保存し（ステップＳ３０９）、バージョン属性情報をバージョン属性情報ファイルとして大容量記憶媒体１０１に保存し（ステップＳ３１０）、データ属性情報をデータ属性情報ファイルとして大容量記憶媒体１０１に保存した後に（ステップＳ３１１）、保存データリストエントリ

22

```
                ；媒体識別番号ファイル
                ；保存データリストファイル
```

を追加して（ステップＳ３１２）、処理を終了する。

【００６５】次に、図３のステップＳ３０７に示したバージョン属性情報の作成処理についてさらに具体的に説明する。図４は、図３のステップＳ３０７に示したバージョン属性情報の作成処理手順を示すフローチャートである。同図に示すように、まず最初に、内部タイマ１０５から現在時刻を取得し（ステップＳ４０１）、内部記憶媒体１０４から最新タイマＩＤを取得する（ステップＳ４０２）。

【００６６】その後、対象コンテンツすべてに対してコンテンツ属性情報を作成するとともに（ステップＳ４０３）、バージョン番号、現在時刻、タイマＩＤ、コンテンツ数、すべてのコンテンツ属性情報などを含むバージョン属性情報を作成する（ステップＳ４０４）。

【００６７】そして、バージョン属性情報に対して改ざん検知コードの計算処理をおこない、バージョン属性ＭＡＣを取得し（ステップＳ４０５）、取得したバージョン属性ＭＡＣをバージョン属性情報に付与して（ステップＳ４０６）、処理を終了する。なお、この改ざん検知コードの計算処理としては、保存するデータに対してハッシュ値を計算するとともに、内部記憶媒体１０４から装置暗号鍵を取得し、ハッシュ値を装置暗号鍵で暗号化してメッセージ認証子とする処理をおこなう。

【００６８】図５は、上記ステップＳ４０３に示したコンテンツ属性情報の作成処理手順を示すフローチャートである。同図に示すように、コンテンツ情報を作成する際には、まず最初に受け取ったデータに対して改ざん検知コードの計算処理をおこない、コンテンツ属性ＭＡＣを取得する（ステップＳ５０１）。

【００６９】そして、内部タイマ１０５から現在時刻を取得し（ステップＳ５０２）、内部記憶媒体１０４から最新タイマＩＤを取得して（ステップＳ５０３）、対象データのコンテンツ番号、現在時刻、タイマＩＤ、対象データを保存する際のファイル名、対象データのサイズおよびコンテンツ属性ＭＡＣなどを含むコンテンツ属性情報を作成する（ステップＳ５０４）。

【００７０】次に、図３のステップＳ３０８に示したデータ属性情報の作成処理について説明する。図６は、図３のステップＳ３０８に示したデータ属性情報の作成処理手順を示すフローチャートである。

【００７１】同図に示すように、まず最初に内部記憶媒体１０４から最新データ識別番号を取得し（ステップＳ

６０１）、最新データ識別番号を１増加させて内部記憶媒体１０４に記録し（ステップＳ６０２）、対象データのバージョン属性情報からバージョン属性ＭＡＣなどの簡易バージョン属性情報を取得する（ステップＳ６０３）。

【００７２】そして、最新データ識別番号、データ属性コード、作成日時情報、最終更新日時情報、簡易バージョン属性情報などを含むデータ属性情報を作成した後（ステップＳ６０４）、このデータ属性情報に対して改ざん検知コードの計算処理をおこなってデータ属性ＭＡＣを取得し（ステップＳ６０５）、取得したデータ属性ＭＡＣをデータ属性情報に付与する（ステップＳ６０６）。

【００７３】次に、図３のステップＳ３１２に示した保存データリストエントリの追加処理についてさらに詳細に説明する。図７は、図３のステップＳ３１２に示した保存データリストエントリの追加処理手順を示すフローチャートである。

【００７４】同図に示すように、まず大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ７０１）、保存データリストに、データ識別番号、データ属性コードおよびデータ属性ＭＡＣなどを含む新しいデータエントリを追加する（ステップＳ７０２）。

【００７５】そして、保存データリストに対して改ざん検知コードの計算処理をおこなってリストＭＡＣを取得し（ステップＳ７０３）、このリストＭＡＣを保存データリストに付与し（ステップＳ７０４）、保存データリストを大容量記憶媒体１０１に保存した後に（ステップＳ７０５）、リストＭＡＣをもとに内部記憶媒体１０４の媒体認証コードリストの対象エントリを更新する（ステップＳ７０６）。

【００７６】次に、図３～図７において説明した新規データの保存処理の具体例について説明する。図８は、図３～図７において説明した新規データの保存処理の一例を示す説明図である。なおここでは、データ属性コードが「原本」であり、コンテンツ名がそれぞれ「chapter1.doc」および「chapter2.doc」であるコンテンツ１およびコンテンツ２からなる新規データを保存する場合を示すこととする。

【００７７】同図に示すように、原本性保証電子保存装置１００に新規に保存されるコンテンツ１および２についてハッシュ値をそれぞれ計算し、計算したハッシュ値を装置暗号鍵で暗号化してコンテンツ属性ＭＡＣを取得する。そして、このコンテンツ属性ＭＡＣを含めたコンテンツ属性情報を作成し、作成したコンテンツ属性情報を含むバージョン属性情報を作成する。

【００７８】その後、このバージョン属性情報からハッシュ値を計算し、計算したハッシュ値を装置暗号鍵で暗号化してバージョン属性ＭＡＣを取得して、取得したバージョン属性ＭＡＣをバージョン属性情報に追加する。

【００７９】また、このバージョン属性ＭＡＣを含むデータ属性情報を作成し、作成したデータ属性情報からハッシュ値を計算し、計算したハッシュ値を装置暗号鍵で暗号化してデータ属性ＭＡＣを取得して、取得したデータ属性ＭＡＣをデータ属性情報に付加する。

【００８０】そして、コンテンツ１および２、バージョン属性情報およびデータ属性情報をそれぞれデータファイル、バージョン属性情報ファイルおよびデータ属性情報ファイルとして大容量記憶媒体１０１に格納するとともに、保存データリストの内容を更新する。

【００８１】上記図３～図８に示した一連の処理をおこなうことにより、複数のコンテンツからなる保存データを原本性を保証しつつ大容量記憶媒体１０１に新規保存することができる。

【００８２】次に、大容量記憶媒体１０１のマウント処理について説明する。図９は、図１に示した大容量記憶媒体１０１のマウント処理手順を示すフローチャートである。同図に示すように、まず最初に装着された大容量記憶媒体１０１がフォーマットされているか否かを調べ（ステップＳ９０１）、フォーマットされていない場合には（ステップＳ９０１肯定）、大容量記憶媒体１０１をフォーマットする（ステップＳ９０２）。

【００８３】具体的には、媒体を初期化し、内部記憶媒体１０４から媒体認証コードリストを取得し、媒体認証コードリストから最新の媒体識別番号を取得し、媒体識別番号を１増加させた新しい媒体識別番号を大容量記憶媒体１０１に記録し、内部記憶媒体１０４の媒体認証コードリストに新しい媒体識別番号のエントリを追加する（リストＭＡＣなし）という手順で大容量媒体１０１をフォーマットする。

【００８４】そして、装着された大容量記憶媒体がフォーマット済みの場合（ステップＳ９０１否定）またはステップＳ９０２によるフォーマット処理を終了した場合には、保存データリストファイルを改ざん検知読み出し処理する（ステップＳ９０３）。

【００８５】具体的には、対象ファイルを読み出し、対象ファイルに記録されたメッセージ認証子とデータを分離し、データに対してハッシュ値を計算し、内部記憶媒体１０４から装置暗号鍵を取得し、装置復号鍵でメッセージ認証子を復号して検証用ハッシュ値とし、先のハッシュ値が検証用ハッシュ値と一致しない場合には改ざんされたものと判断する処理をおこなう。

【００８６】そして、改ざんがなされていると判断された場合には（ステップＳ９０４肯定）、エラー処理をおこない（ステップＳ９１０）、改ざんがなされていないと判断された場合には（ステップＳ９０４否定）、大容量記憶媒体１０１から媒体識別番号を取得し（ステップＳ９０５）、この媒体識別番号に該当するメッセージ認証子（リストＭＡＣ）を内部記憶媒体１０４から取得するとともに（ステップＳ９０６）、保存データリストフ

ファイルに付与されたメッセージ認証子を取得する（ステップＳ９０７）。

【００８７】そして、両メッセージ認証子が同じであるならば（ステップＳ９０８否定）、認証に成功（ステップＳ９０９）したものとして正常終了し、両メッセージ認証子が異なる場合には（ステップＳ９０８肯定）、エラー処理する（ステップＳ９１０）。

【００８８】上記一連の処理をおこなうことにより、大容量記憶媒体１０１が取り外し可能な場合に、この大容量記憶媒体１０１のマウント時にその正当性を検証することができる。

【００８９】次に、図１に示した原本性保証電子保存装置１００によるデータ読み出し処理について説明する。図１０および図１１は、図１に示した原本性保証電子保存装置１００によるデータ読み出し処理手順を示すフローチャートである。

【００９０】同図に示すように、まず最初に大容量記憶媒体１０１がマウントされているか否かを調べ（ステップＳ１００１）、大容量記憶媒体１０１がマウントされていない場合には（ステップＳ１００１肯定）、エラー処理をおこなって（ステップＳ１００２）処理を終了する。

【００９１】これに対して、大容量記憶媒体１０１がマウントされている場合には（ステップＳ１００１否定）、大容量記憶媒体１０１の保存データリストファイルを読み出し（ステップＳ１００３）、この保存データリストから対象データのエントリを取得する（ステップＳ１００４）。

【００９２】そして、対象データのエントリが存在するか否かを調べ（ステップＳ１００５）、該当するエントリが存在しない場合には（ステップＳ１００５肯定）、大容量記憶媒体１０１から対象データファイルを読み出し（ステップＳ１００６）、読み出しデータを外部システムに送出して（ステップＳ１００７）、処理を終了する。

【００９３】これに対して、対象データのエントリが存在する場合には（ステップＳ１００５否定）、大容量記憶媒体１０１から対象データのデータ属性情報ファイルを読み出し（ステップＳ１００９）、データ属性情報に対して改ざん検知コード検証処理をおこなう（ステップＳ１０１０）。

【００９４】そして、改ざんされているか否かを確認し（ステップＳ１０１１）、改ざんされている場合には（ステップＳ１０１１肯定）、エラー処理をおこなった後に処理を終了し（ステップＳ１００２）、改ざんされていない場合には（ステップＳ１０１１否定）、取得したデータ属性情報からデータ属性ＭＡＣを取得し（ステップＳ１０１２）、取得したデータ属性ＭＡＣと先のデータ属性ＭＡＣとが一致するか否かを確認する（ステップＳ１０１３）。

【００９５】その結果、両者が一致しない場合には（ステップＳ１０１３肯定）、エラー処理をおこなった後に処理を終了し（ステップＳ１００２）、両者が一致する場合には（ステップＳ１０１３否定）、外部システムがバージョン番号を指定しているか否かを確認する（ステップＳ１０１４）。そして、バージョン番号が指定されていない場合には（ステップＳ１０１４肯定）、対象バージョンを最新版とする（ステップＳ１０１５）。

【００９６】その後、データ属性情報から対象バージョンのバージョン属性ＭＡＣを取得し（ステップＳ１０１６）、大容量記憶媒体１０１から対象バージョンのバージョン属性情報ファイルを読み出して（ステップＳ１０１７）、バージョン属性情報ファイルに対して改ざん検知コード検証処理をおこない（ステップＳ１０１８）、改ざんされているか否かを確認する（ステップＳ１０１９）。

【００９７】その結果、改ざんされている場合には（ステップＳ１０１９肯定）、エラー処理をおこなった後に処理を終了し（ステップＳ１００２）、改ざんされていない場合には（ステップＳ１０１９否定）、取得したバージョン属性情報からバージョン属性ＭＡＣを取得し（ステップＳ１０２０）、取得したバージョンＭＡＣと先のバージョン属性ＭＡＣが一致するか否かを調べる（ステップＳ１０２１）。

【００９８】そして、両者が一致しない場合には（ステップＳ１０２１肯定）、エラー処理をおこなった後に処理を終了し（ステップＳ１００２）、両者が一致する場合には（ステップＳ１０２１否定）、大容量記憶媒体１０１から対象データの対象バージョンの対象コンテンツのデータファイルを読み出す（ステップＳ１０２２）。

【００９９】なお、対象データファイルが存在しない場合には（ステップＳ１０２３肯定）、対象バージョンの前のバージョンの対象コンテンツのデータファイルを読み出す（ステップＳ１０２４）。

【０１００】その後、読み出したデータに対してハッシュ値を計算し（ステップＳ１０２５）、バージョン属性情報から対象コンテンツのコンテンツ属性ＭＡＣを取得して（ステップＳ１０２６）、コンテンツ属性ＭＡＣを装置復号鍵で復号してハッシュ値を取得する（ステップＳ１０２７）。

【０１０１】そして、取得したハッシュ値と先に計算したハッシュ値とが一致するか否かを確認し（ステップＳ１０２８）、一致しない場合には（ステップＳ１０２８肯定）、エラー処理をおこなって処理を終了する（ステップＳ１００２）。これに対して、取得したハッシュ値と先に計算したハッシュ値とが一致する場合には（ステップＳ１０２８否定）、読み出したデータを外部システムに送出する（ステップＳ１０２９）。

【０１０２】上記一連の処理をおこなうことにより、外部システムからデータ読み出し要求を受け取ると、対象

データの正当性を検証した後に、該当するデータを外部システムに送出することができる。

【０１０３】次に、図１に示した原本性保証電子保存装置１００による謄本作成処理について説明する。図１２～図１５は、図１に示した原本性保証電子保存装置１００による謄本作成処理手順を示すフローチャートである。

【０１０４】この原本性保証電子保存装置１００では、「原本」の属性を持つデータに対して外部から複製要求を受け取ると、対象データファイルと、それに関連づけられたデータ属性情報ファイルおよびバージョン属性情報ファイルとを複写し、新たなデータ属性ファイルには「謄本」のデータ属性コードを付加する。

【０１０５】また、謄本の作成先が別の原本性保証電子保存装置の場合には、作成先の原本性保証電子保存装置にログインしてファイルを転送する。なお、ログインの手順については外部システムが原本性保証電子保存装置にログインする場合と同様の手順でおこなう。さらに、原本性保証電子保存装置間でやりとりされるデータの保護についても、外部システムと原本性保証電子保存装置との間でやりとりするデータの保護方法と同じである。

【０１０６】また、この謄本作成処理においても、データ保存処理と同様に保存データリストの更新をおこない、データ転送先の原本性保証電子保存装置では転送受け入れ処理がおこなわれる。

【０１０７】バージョン番号が指定されると、対象バージョンのデータファイルのみがコピーされバージョン番号が指定されない場合には、全バージョンがコピーされ、バージョン番号として「－１」が指定されると、最新バージョンのみがコピーされる。

【０１０８】具体的には、図１２～図１５に示すように、まず最初に大容量記憶媒体１０１がマウントされているか否かを調べ（ステップＳ１１０１）、マウントされていない場合には（ステップＳ１１０１肯定）、エラー処理をおこなった後に（ステップＳ１１０２）処理を終了する。

【０１０９】これに対して、マウントされている場合には（ステップＳ１１０１否定）、大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ１１０３）、保存データリストから対象データのエントリを取得する（ステップＳ１１０４）。なお、対象データのエントリが存在しない場合には（ステップＳ１１０５肯定）、エラー処理をおこなった後に処理を終了する（ステップＳ１１０２）。

【０１１０】その後、エントリからデータ属性コードを取得し（ステップＳ１１０６）、データ属性コードが「原本」であるか否かを調べ（ステップＳ１１０７）、「原本」でない場合には（ステップＳ１１０７肯定）、エラー処理をおこなった後に処理を終了する（ステップＳ１１０２）。

【０１１１】これに対して、データ属性コードが「原本」である場合には（ステップＳ１１０７否定）、エントリからデータ属性ＭＡＣを取得し（ステップＳ１１０８）、対象データのデータ属性情報ファイルを読み出し（ステップＳ１１０９）、データ属性情報に対して改ざん検知コード検証処理をおこない（ステップＳ１１１０）、改ざんされているか否かを確認する（ステップＳ１１１１）。

【０１１２】その結果、改ざんされている場合には（ステップＳ１１１１肯定）、エラー処理をおこなった後に処理を終了し（ステップＳ１１０２）、改ざんされていない場合には（ステップＳ１１１１否定）、データ属性情報からデータ属性ＭＡＣを取得し（ステップＳ１１１２）、取得したデータ属性ＭＡＣと先のデータ属性ＭＡＣとが一致するか否かを確認し（ステップＳ１１１３）、両者が一致しない場合には（ステップＳ１１１３肯定）、エラー処理をおこなった後に処理を終了する（ステップＳ１１０２）。

【０１１３】これに対して、両者が一致する場合には（ステップＳ１１１３否定）、バージョン番号が指定されているか否かを確認し（ステップＳ１１１４）、このバージョン番号が指定されていない場合には（ステップＳ１１１４肯定）、対象バージョンを全バージョンとする（ステップＳ１１１５）。また、バージョン番号が「－１」の場合には（ステップＳ１１１６肯定）、対象バージョンを最新版とする（ステップＳ１１１７）。

【０１１４】その後、データ属性情報から対象バージョンのバージョン属性ＭＡＣを取得し（ステップＳ１１１８）、対象バージョンのバージョン属性情報ファイルを読み出し（ステップＳ１１１９）、バージョン属性情報に対して改ざん検知コード検証処理をおこなって（ステップＳ１１２０）、改ざんされているか否かを確認する（ステップＳ１１２１）。

【０１１５】その結果、改ざんされている場合には（ステップＳ１１２１肯定）、エラー処理をおこなった後に処理を終了し（ステップＳ１１０２）、改ざんされていない場合には（ステップＳ１１２１否定）、バージョン属性情報からバージョン属性ＭＡＣを取得する（ステップＳ１１２２）。

【０１１６】そして、取得したバージョン属性ＭＡＣが先のバージョン属性ＭＡＣと一致するか否かを確認し（ステップＳ１１２３）、両者が一致しない場合には（ステップＳ１１２３肯定）、エラー処理をおこなった後に処理を終了する（ステップＳ１１０２）。

【０１１７】これに対して、両者が一致する場合には（ステップＳ１１２３否定）、対象バージョンのコンテンツデータファイルを特定し（ステップＳ１１２４）、バージョン属性情報に含まれる全コンテンツのコンテンツ属性ＭＡＣを取得して（ステップＳ１１２５）、大容量記憶媒体１０１から対象コンテンツデータファイルを

読み出す（ステップＳ１１２６）。

【０１１８】その後、対象コンテンツデータについてハッシュ値を計算し（ステップＳ１１２７）、内部記憶媒体１０４から装置復号鍵を取得して（ステップＳ１１２８）、コンテンツ属性ＭＡＣを装置復号鍵で復号して検証用ハッシュ値を計算し（ステップＳ１１２９）、先のハッシュ値と検証用ハッシュ値が一致するか否かを確認する（ステップＳ１１３０）。

【０１１９】その結果、両者が一致しない場合には（ステップＳ１１３０肯定）、エラー処理をおこなった後に処理を終了し（ステップＳ１１０２）、両者が一致する場合には（ステップＳ１１３０否定）、作成先が同じ原本性保証電子保存装置内であるか否かを確認する（ステップＳ１１３１）。

【０１２０】そして、作成先が同じ原本性保証電子保存装置内である場合には（ステップＳ１１３１肯定）、内部記憶媒体１０４から最新データ識別番号を取得し（ステップＳ１１３２）、最新データ識別番号を１増加させて内部記憶媒体１０４に記録する（ステップＳ１１３３）。

【０１２１】その後、対象データの対象バージョンのコンテンツデータファイルを作成先にコピーし（ステップＳ１１３４）、対象データの対象バージョンのバージョン属性情報ファイルを作成先にコピーし（ステップＳ１１３５）、対象データのデータ属性情報ファイルを作成先にコピーする（ステップＳ１１３６）。

【０１２２】そして、作成先のデータ属性情報ファイルを読み出し処理し（ステップＳ１１３７）、データ属性情報のデータ属性コードを「謄本」に変更し（ステップＳ１１３８）、データ属性情報の参照原本識別番号に現在のデータ識別番号を設定する（ステップＳ１１３９）。

【０１２３】また、データ属性情報のデータ識別番号を新しいデータ識別番号に変更し（ステップＳ１１４０）、内部タイマ１０５から現在時刻を取得し（ステップＳ１１４１）、データ属性情報に謄本作成履歴（ユーザ名、現在時刻、タイマＩＤ等）を追加する（ステップＳ１１４２）。

【０１２４】そして、データ属性情報に対して改ざん検知コード計算処理をおこなってデータ属性ＭＡＣを取得し（ステップＳ１１４３）、データ属性情報にデータ属性情報ＭＡＣを付与し（ステップＳ１１４４）、データ属性情報を大容量記憶媒体１０１にデータ属性情報ファイルとして保存して（ステップＳ１１４５）、保存データリストファイルを追加処理する（ステップＳ１１４６）。

【０１２５】また、上記ステップＳ１１３１において、作成先が同じ原本性保証電子保存装置内でない場合には（ステップＳ１１３１否定）、作成先の原本性保証電子保存装置にログインし（ステップＳ１１４６）、対象データの対象バージョンのコンテンツデータを作成先の原本性保証電子保存装置に謄本作成モードで転送する（ステップＳ１１４７）。

【０１２６】また、対象データの対象バージョンのバージョン属性情報を作成先の原本性保証電子保存装置に謄本作成モードで転送し（ステップＳ１１４８）、対象データのデータ属性情報を作成先の原本性保証電子保存装置に謄本作成モードで転送して（ステップＳ１１４９）、作成先の原本性保証電子保存装置からログアウトする（ステップＳ１１５０）。

【０１２７】次に、図１に示した原本性保証電子保存装置１００のデータ移動処理について説明する。図１６および図１７は、図１に示した原本性保証電子保存装置１００のデータ移動処理手順を示すフローチャートである。なお、ここでは移動を全バージョン一括でしかおこなえないものとする。

【０１２８】同図に示すように、まず最初に大容量記憶媒体１０１がマウントされているか否かを判断し（ステップＳ１３０１）、マウントされていない場合には（ステップＳ１３０１肯定）、エラー処理をおこなった後に（ステップＳ１３０２）処理を終了する。

【０１２９】これに対して、大容量記憶媒体１０１がマウントされている場合には（ステップＳ１３０１否定）、大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ１３０３）、保存データリストから対象データのエントリを取得する（ステップＳ１３０４）。なお、対象データのエントリが存在しない場合には（ステップＳ１３０５肯定）、対象データのデータファイルを移動モードで転送した後に（ステップＳ１３０６）、対象データのデータファイルを大容量記憶媒体１０１から削除して（ステップＳ１３０７）、処理を終了する。

【０１３０】そして、対象データのエントリが存在する場合には（ステップＳ１３０５否定）、エントリからデータ属性ＭＡＣを取得し（ステップＳ１３０８）、対象データのデータ属性情報ファイルを読み出し（ステップＳ１３０９）、データ属性情報に対して改ざん検知コード検証処理をおこない（ステップＳ１３１０）、改ざんされているか否かを確認する（ステップＳ１３１１）。

【０１３１】その結果、改ざんされている場合には（ステップＳ１３１１肯定）、エラー処理をおこなった後に処理を終了し（ステップＳ１３０２）、改ざんされていない場合には（ステップＳ１３１１否定）、データ属性情報からデータ属性ＭＡＣを取得し（ステップＳ１３１２）、取得したデータ属性ＭＡＣと先のデータ属性ＭＡＣが一致するか否かを確認し（ステップＳ１３１３）、両者が一致しない場合には（ステップＳ１３１３肯定）、エラー処理をおこなった後に処理を終了する（ステップＳ１３０２）。

【０１３２】これに対して、両者が一致する場合には

31

（ステップＳ１３１３否定）、データ属性情報から全バージョンのバージョン属性ＭＡＣを取得し（ステップＳ１３１４）、全バージョンのバージョン属性情報ファイルを読み出し（ステップＳ１３１５）、各バージョン属性情報に対して改ざん検知コード検証処理をおこない（ステップＳ１３１６）、改ざんされているか否かを確認する（ステップＳ１３１７）。

【０１３３】その結果、改ざんされている場合には（ステップＳ１３１７肯定）、エラー処理をおこなった後に処理を終了し（ステップＳ１３０２）、改ざんされていない場合には（ステップＳ１３１７否定）、各バージョン属性情報からバージョン属性ＭＡＣを取得し（ステップＳ１３１８）、取得した各バージョン属性ＭＡＣが先の各バージョン属性ＭＡＣと一致するか否かを確認し（ステップＳ１３１９）、両者が一致しない場合には（ステップＳ１３１９肯定）、エラー処理をおこなった後に処理を終了する（ステップＳ１３０２）。

【０１３４】これに対して、両者が一致する場合には（ステップＳ１３１９否定）、全バージョン属性情報に含まれる全コンテンツのコンテンツ属性ＭＡＣを取得し（ステップＳ１３２０）、大容量記憶媒体１０１から対象となる全コンテンツデータファイルを読み出す（ステップＳ１３２１）。

【０１３５】その後、各コンテンツデータについてハッシュ値を計算し（ステップＳ１３２２）、内部記憶媒体１０４から装置復号鍵を取得して（ステップＳ１３２３）、各コンテンツ属性ＭＡＣを装置復号鍵で復号化して検証ハッシュ値を計算し（ステップＳ１３２４）、先のハッシュ値と各検証ハッシュ値が一致するか否かを確認する（ステップＳ１３２５）。

【０１３６】その結果、両者が一致しない場合には（ステップＳ１３２５肯定）、エラー処理をおこなった後に処理を終了し（ステップＳ１３０２）、両者が一致する場合には（ステップＳ１３２５否定）、移動先の原本性保証電子保存装置にログインする（ステップＳ１３２６）。

【０１３７】そして、全コンテンツデータを移動先の原本性保証電子保存装置に移動モードで転送し（ステップＳ１３２７）、全バージョン属性情報を移動先の原本性保証電子保存装置に移動モードで転送し（ステップＳ１３２８）、データ属性情報を移動先の原本性保証電子保存装置に移動モードで転送する（ステップＳ１３２９）。

【０１３８】その後、対象データの全コンテンツデータファイルを削除し（ステップＳ１３３０）、対象データの全バージョン属性情報ファイルを削除し（ステップＳ１３３１）、対象データのデータ属性情報ファイルを削除し（ステップＳ１３３２）、移動したデータに対して保存データリストエントリの削除処理をおこなった後に（ステップＳ１３３３）、移動先の原本性保証電子保存装置からログアウトする（ステップＳ１３３４）。

32

【０１３９】図１８は、図１７のステップＳ１３３３で示した保存データリストエントリの削除処理手順を示すフローチャートである。同図に示すように、保存データリストエントリを削除する際には、大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ１４０１）、保存データリストから対象エントリを削除する（ステップＳ１４０２）。

【０１４０】そして、新しい保存データリストに対してハッシュ値を計算し（ステップＳ１４０３）、内部記憶媒体１０４から装置暗号鍵を取得して（ステップＳ１４０４）、装置暗号鍵でハッシュ値を暗号化してリストＭＡＣを取得する（ステップＳ１４０５）。

【０１４１】その後、新しい保存データリストにリストＭＡＣを付与し（ステップＳ１４０６）、保存データリストを大容量記憶媒体１０１に保存データリストファイルとして保存した後に（ステップＳ１４０７）、内部記憶媒体１０４の媒体認証コードリストを新しいリストＭＡＣで更新する（ステップＳ１４０８）。

【０１４２】次に、移動先の原本性保証電子保存装置における転送受け入れ処理について説明する。図１９および図２０は、移動先の原本性保証電子保存装置における転送受け入れ処理手順を示すフローチャートである。

【０１４３】同図に示すように、まず最初に大容量記憶媒体１０１がマウントされているか否かを判断し（ステップＳ１５０１）、マウントされていない場合には（ステップＳ１５０１肯定）、エラー処理をおこなって処理を終了する（ステップＳ１５０２）。

【０１４４】これに対して、大容量記憶媒体１０１がマウントされている場合には（ステップＳ１５０１否定）、謄本作成モードであるか否かを確認し（ステップＳ１５０３）、謄本作成モードである場合には（ステップＳ１５０３肯定）、大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ１５０４）、受け取った全コンテンツデータに対して改ざん検知コード計算処理をおこなってコンテンツ属性ＭＡＣを取得し（ステップＳ１５０５）、受け取ったバージョン属性情報の中のコンテンツ属性ＭＡＣを更新する（ステップＳ１５０６）。

【０１４５】その後、新しいバージョン属性情報に対して改ざん検知コード計算処理をおこなってバージョン属性ＭＡＣを取得し（ステップＳ１５０７）、バージョン属性情報にバージョン属性ＭＡＣを付与し（ステップＳ１５０８）、受け取ったデータ属性情報の中のバージョン属性ＭＡＣを更新する（ステップＳ１５０９）。

【０１４６】また、データ属性情報のデータ属性コードを「謄本」に変更し（ステップＳ１５１０）、データ属性情報のデータ識別番号を参照原本識別番号として設定し（ステップＳ１５１１）、内部記憶媒体１０４から最新データ識別番号を取得する（ステップＳ１５１２）。

33

【０１４７】そして、この最新データ識別番号に１を加えた番号で内部記憶媒体１０４の最新データ識別番号を更新し（ステップＳ１５１３）、データ属性情報のデータ識別番号に最新データ識別番号を設定して（ステップＳ１５１４）、データ属性情報に謄本作成履歴を追加する（ステップＳ１５１５）。

【０１４８】そして、新しいデータ属性情報に対して改ざん検知コード計算処理をおこなってデータ属性ＭＡＣを取得し（ステップＳ１５１６）、データ属性情報にデータ属性ＭＡＣを付与し（ステップＳ１５１７）、受け取った全コンテンツデータをデータファイルとして大容量記憶媒体１０１に保存する（ステップＳ１５１８）。

【０１４９】また、データ属性情報を大容量記憶媒体１０１にデータ属性情報ファイルとして保存し（ステップＳ１５１９）、バージョン属性情報を大容量記憶媒体１０１にバージョン属性情報ファイルとして保存して（ステップＳ１５２０）、対象データについて保存データリストエントリ追加処理する（ステップＳ１５２１）。

【０１５０】これに対して、上記ステップＳ１５０３において謄本作成モードではなく移動モードである場合には（ステップＳ１５０３否定）、データ属性情報を受け取ったか否かを確認し（ステップＳ１５２２）、受け取った場合には（ステップＳ１５２２肯定）、このデータ属性情報を大容量記憶媒体１０１に保存する（ステップＳ１５２３）。

【０１５１】そして、大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ１５２４）、受け取った全コンテンツデータに対して改ざん検知コード計算処理をおこなってコンテンツ属性ＭＡＣを取得し（ステップＳ１５２５）、受け取った全バージョン属性情報の中のコンテンツ属性ＭＡＣを更新する（ステップＳ１５２６）。

【０１５２】そして、新しい全バージョン属性情報に対して改ざん検知コード計算処理をおこなってバージョン属性ＭＡＣを取得し（ステップＳ１５２７）、全バージョン属性情報に各バージョン属性ＭＡＣを付与し（ステップＳ１５２８）、受け取ったデータ属性情報の中の全バージョン属性ＭＡＣを更新する（ステップＳ１５２９）。

【０１５３】そして、内部記憶媒体１０４から最新データ識別番号を取得し（ステップＳ１５３０）、この最新データ識別番号に１を加えた番号で内部記憶媒体１０４の最新データ識別番号を更新し（ステップＳ１５３１）、データ属性情報のデータ識別番号に最新データ識別番号を設定し（ステップＳ１５３２）、データ属性情報にデータ移動履歴を追加する（ステップＳ１５３３）。

【０１５４】そして、新しいデータ属性情報に対して改ざん検知コード計算処理をおこなってデータ属性ＭＡＣを取得し（ステップＳ１５３４）、データ属性情報にデータ属性ＭＡＣを付与する（ステップＳ１５３５）。

34

【０１５５】その後、受け取った全コンテンツデータをデータファイルとして大容量記憶媒体１０１に保存し（ステップＳ１５３６）、データ属性情報を大容量記憶媒体１０１にデータ属性情報ファイルとして保存し（ステップＳ１５３７）、全バージョン属性情報を大容量記憶媒体１０１にバージョン属性情報ファイルとして保存し（ステップＳ１５３８）、対象データについて保存データリストエントリ追加処理をおこなう（ステップＳ１５３９）。

【０１５６】次に、図１に示した原本性保証電子保存装置１００によるデータの削除処理について説明する。図２１は、図１に示した原本性保証電子保存装置１００によるデータの削除処理手順を示すフローチャートである。なおここでは、「原本」のデータ属性コードを持つデータは証拠隠滅を防ぐために削除しないこととする。

【０１５７】同図に示すように、まず最初に大容量記憶媒体１０１がマウントされているか否かを判断し（ステップＳ１６０１）、マウントされていない場合には（ステップＳ１６０１肯定）、エラー処理をおこなって（ステップＳ１６０２）処理を終了する。

【０１５８】これに対して、大容量記憶媒体１０１がマウントされている場合には（ステップＳ１６０１否定）、大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ１６０３）、対象データに該当するエントリを取得する（ステップＳ１６０４）。なお、エントリが存在しない場合には（ステップＳ１６０５肯定）、対象データを削除する（ステップＳ１６０６）。

【０１５９】その後、エントリから対象データのデータ属性コードを取得し（ステップＳ１６０７）、このデータ属性コードが「原本」であるか否かを確認する（ステップＳ１６０８）。

【０１６０】そして、データ属性コードが「原本」である場合には（ステップＳ１６０８肯定）、エラー処理をおこなって処理を終了し（ステップＳ１６０２）、「原本」でない場合には（ステップＳ１６０８否定）、対象データについて保存データリストエントリを削除し（ステップＳ１６０９）、対象データの全コンテンツデータファイルを削除し（ステップＳ１６１０）、対象データの全バージョン属性情報ファイルを削除し（ステップＳ１６１１）、対象データのデータ属性ファイルを削除する（ステップＳ１６１２）。

【０１６１】次に、図１に示した原本性保証電子保存装置１００によるデータ属性コードの変更処理について説明する。データ保存処理において、「仮原本」の属性を持つデータを保存することはできるが、この「仮原本」データは単純にデータ属性コードを「原本」に変更することが可能である。

【０１６２】また、「謄本」、「バックアップ仮原

本」、「バックアップ原本」および「バックアップ謄本」の属性を持つデータはそれぞれ属性コードを変更することで元のデータを復旧することができる。

【０１６３】かかる復旧をおこなうと、図２２に示すように、「謄本」が「原本」に復旧され、「バックアップ仮原本」が「仮原本」に復旧され、「バックアップ原本」が「原本」に復旧され、「バックアップ謄本」が「謄本」に復旧される。なお、かかるデータ属性コードを変更するとこれをデータアクセス履歴として記録することとなる。

【０１６４】また、図２３および図２４は、図１に示した原本性保証電子保存装置１００によるデータ属性コードの変更処理手順を示すフローチャートである。同図に示すように、まず最初に大容量記憶媒体１０１がマウントされているか否かを確認し（ステップＳ１８０１）、マウントされていない場合には（ステップＳ１８０１肯定）、エラー処理をおこなって（ステップＳ１８０２）処理を終了する。

【０１６５】これに対して、大容量記憶媒体１０１がマウントされている場合には（ステップＳ１８０１否定）、大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ１８０３）、保存データリストから対象データに該当するエントリを取得する（ステップＳ１８０４）。なお、該当するエントリが存在しない場合には（ステップＳ１８０５肯定）、エラー処理をおこなって（ステップＳ１８０２）処理を終了する。

【０１６６】その後、エントリから現データ属性コードを取得し（ステップＳ１８０６）、新データ属性コードが「仮原本」であり（ステップＳ１８０７肯定）、現データ属性コードが「バックアップ仮原本」である場合には（ステップＳ１８０８否定）、データ属性情報のデータ属性コードを「仮原本」に変更する（ステップＳ１８０９）。

【０１６７】なお、ステップＳ１８０８で現データ属性コードが「バックアップ仮原本」でない場合には（ステップＳ１８０８肯定）、エラー処理をおこなって処理を終了する（ステップＳ１８０２）。

【０１６８】また、新データ属性コードが「仮原本」でない場合には（ステップＳ１８０７否定）、この新データ属性コードが「原本」であるか否かを調べ（ステップＳ１８１０）、この新データ属性コードが「原本」である場合には（ステップＳ１８１０肯定）、現データ属性コードが「バックアップ仮原本」または「仮原本」であるか否かを調べる（ステップＳ１８１１）。

【０１６９】その結果、現データ属性コードが「バックアップ仮原本」または「仮原本」である場合には（ステップＳ１８１１否定）、データ属性情報のデータ属性コードを「原本」に変更する（ステップＳ１８１２）。

【０１７０】なお、ステップＳ１８１１で現データ属性コードが「バックアップ原本」または「仮原本」でない場合には（ステップＳ１８１１肯定）、エラー処理をおこなって処理を終了する（ステップＳ１８０２）。

【０１７１】また、新データ属性コードが「原本」でない場合には（ステップＳ１８１０否定）、この新データ属性コードが「謄本」であるか否かを調べ（ステップＳ１８１３）、この新データ属性コードが「謄本」である場合には（ステップＳ１８１３肯定）、現データ属性コードが「バックアップ謄本」であか否かを調べ（ステップＳ１８１４）、「バックアップ謄本」である場合には（ステップＳ１８１４否定）、データ属性情報のデータ属性コードを「謄本」に変更する（ステップＳ１８１５）。

【０１７２】なお、ステップＳ１８１４で現データ属性コードが「バックアップ謄本」でない場合には（ステップＳ１８１４肯定）、エラー処理をおこなって処理を終了する（ステップＳ１８０２）。

【０１７３】そして、これらの変更を終えたならば、タイマ１０５から現在時刻を取得し（ステップＳ１８１６）、データ属性情報にデータ属性コード変更履歴を追加して（ステップＳ１８１７）、新しいデータ属性情報を改ざん検知コード計算処理をおこなってデータ属性ＭＡＣを取得して（ステップＳ１８１８）、データ属性情報にデータ属性ＭＡＣを付与する（ステップＳ１８１９）。

【０１７４】その後、データ属性情報を大容量記憶媒体１０１にデータ属性情報ファイルとして保存し（ステップＳ１８２０）、対象データについて保存データリストエントリの更新処理をおこなって（ステップＳ１８２１）、処理を終了する。

【０１７５】図２５は、図２４のステップＳ１８２１に示した保存データリストエントリの更新処理手順を示すフローチャートである。同図に示すように、保存データリストエントリの更新処理では、大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ１９０１）、保存データリストの対象データに該当するエントリを更新する（ステップＳ１９０２）。

【０１７６】そして、保存データリストに対してハッシュ値を計算し（ステップＳ１９０３）、内部記憶媒体１０４から装置暗号鍵を取得して（ステップＳ１９０４）、ハッシュ値を装置暗号鍵で暗号化してリストＭＡＣを取得する（ステップＳ１９０５）。

【０１７７】そして、保存データリストにリストＭＡＣを付与し（ステップＳ１９０６）、保存データリストを大容量記憶媒体１０１に保存して（ステップＳ１９０７）、内部記憶媒体１０４の媒体認証コードリスト内の該当するリストＭＡＣを更新する（ステップＳ１９０８）。

【０１７８】次に、図１に示した原本性保証電子保存装置１００によるデータのバージョンアップ処理について説明する。このデータバージョンアップ処理では、「原

本」および「仮原本」のデータ属性コードを持つデータに対しては編集を許可しないが、バージョンアップについては許可することとしている。このように、バージョンアップのみを許可することにより、以前のデータが失われず、電子データの編集履歴が分かるため、その証明力が高まることになる。

【０１７９】また、この原本性保証電子保存装置１００では、「謄本」およびバックアップのデータについては、追記や編集を許可しない。その理由は、データの訂正や修正は、原本に対して施すべきものであり、コピーやバックアップに対して施すべきものではないからである。

【０１８０】また、バージョンを上げる際に、編集していないコンテンツデータファイルについては、前のバージョンのコンテンツデータファイルをそのまま参照することとし、あるバージョンを指定した謄本作成は、そのバージョンにコンテンツデータファイルがない場合には、前のバージョンを辿ってコンテンツデータファイルをコピーすることとする。

【０１８１】かかるバージョンアップ処理は、対象となるデータのデータ識別番号および対象コンテンツ番号を指定してコンテンツデータが外部から渡されるか、若しくは、そのコンテンツデータを削除する要求を渡すこととする。

【０１８２】図２６は、図１に示した原本性保証電子保存装置１００によるデータのバージョンアップ処理手順を示すフローチャートである。同図に示すように、大容量記憶媒体１０１がマウントされている場合には（ステップＳ２００１否定）、大容量記憶媒体１０１から保存データリストファイルを読み出す（ステップＳ２００３）。

【０１８３】そして、読み出した保存データリストから対象データのエントリを取得し（ステップＳ２００４）、エントリに記録されているデータ属性コードが「原本」または「仮原本」であるか否かが判断される（ステップＳ２００５）。なお「原本」または「仮原本」でない場合や（ステップＳ２００５肯定）、大容量記憶媒体１０１がマウントされていない場合には（ステップＳ２００１肯定）、エラー処理をおこなった後に（ステップＳ２００２）処理を終了する。

【０１８４】そして、データ属性コードが「原本」または「仮原本」である場合には（ステップＳ２００５否定）、エントリの中からデータ属性ＭＡＣを取得するとともに（ステップＳ２００６）、対象データに対応したデータ属性情報ファイルを読み出し（ステップＳ２００７）、データ属性情報からデータ属性ＭＡＣを取得し（ステップＳ２００８）、両属性ＭＡＣが一致するか否かを確認する（ステップＳ２００９）。

【０１８５】そして、両属性ＭＡＣが一致しない場合には（ステップＳ２００９肯定）、エラー処理をおこなって（ステップＳ２００２）処理を終了し、両属性ＭＡＣが一致する場合には（ステップＳ２００９否定）、データ属性情報に対して改ざん検知コード検証処理をおこない（ステップＳ２０１０）、改ざんされているか否かを確認し（ステップＳ２０１１）、改ざんされている場合には（ステップＳ２０１１肯定）、エラー処理をおこなって（ステップＳ２００２）処理を終了する。

【０１８６】これに対して、改ざんされていない場合には（ステップＳ２０１１否定）、読み出したデータ属性情報から最新バージョン番号を取得し（ステップＳ２０１２）、最新バージョン番号に１を加えて現バージョン番号とし（ステップＳ２０１３）、外部から受け取ったデータをコンテンツデータファイルとして大容量記憶媒体１０１に保存する（ステップＳ２０１４）。

【０１８７】そして、現バージョンのバージョン属性情報作成処理をおこない（ステップＳ２０１５）、バージョン属性情報をバージョン属性情報ファイルとして大容量記憶媒体１０１に保存し（ステップＳ２０１６）、現バージョンのバージョン属性情報ファイルをもとにデータ属性情報更新処理をおこなう（ステップＳ２０１７）。

【０１８８】そして、データ属性情報をデータ属性情報ファイルとして大容量記憶媒体１０１に保存し（ステップＳ２０１８）、保存データリストファイルの対象データに該当するエントリの内容を新しいデータ属性情報をもとに更新し（ステップＳ２０１９）、保存データリストエントリを更新処理する（ステップＳ２０２０）。

【０１８９】次に、図１に示した原本性保証電子保存装置１００によるデータの編集処理について説明する。この原本性保証電子保存装置１００では、「仮原本」および「原本」のデータについては修正履歴を残すことで証明力を高めるために、データに対する編集要求を拒否し、また「謄本」やバックアップは、本来編集すべき対象ではないので、同様に編集要求を拒否する。このため、結果的に「一般」のデータのみが編集可能となる。

【０１９０】図２７は、図１に示した原本性保証電子保存装置１００によるデータの編集処理手順を示すフローチャートである。同図に示すように、大容量記憶媒体１０１がマウントされている場合には（ステップＳ２１０１否定）、大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ２１０３）、保存データリストから対象データに該当するエントリを取得する（ステップＳ２１０４）。

【０１９１】なお、エントリが取得できない場合や（ステップＳ２１０５否定）、大容量記憶媒体１０１がマウントされていない場合には（ステップＳ２１０１肯定）、エラー処理をおこなって処理を終了する（ステップＳ２１０２）。

【０１９２】そして、エントリが取得された場合には（ステップＳ２１０５肯定）、対象データのデータファ

39

イルの編集をおこなって（ステップＳ２１０６）、処理を終了する。

【０１９３】次に、図１に示した原本性保証電子保存装置１００へのクライアント（ホスト計算機１１０）からのログイン処理について説明する。この原本性保証電子保存装置１００にデータを保存したりデータを読み出す前に、クライアントは原本性保証電子保存装置１００にログインしなければならない。

【０１９４】このログイン処理としては、従来から知られているＩＣカードを用いる技術を採用することもできるが、本実施の形態では、パスワードによる一般的なチャレンジ　レスポンス認証処理をおこなっている。

【０１９５】たとえば、電子申請システムなどの場合には、エンドユーザが電子申請書類を電子申請サーバに送付し、電子申請サーバが原本性保証電子保存装置にログインして電子申請書類を原本性保証電子保存装置に保存するという運用が考えられるが、かかる場合に、ログインするのは常に電子申請サーバであるため、原本性保証電子保存装置に保存されたデータの作成者や更新者がすべて電子申請サーバになるものと考えられる。

【０１９６】そこで、本実施の形態では、ログインそのものは電子申請サーバがおこなうが、その後の処理を誰の代理でおこなっているのかを設定できるようにしている。また、原本性保証電子保存装置に保存されるデータについて、作成者や更新者の名前として、この設定されたユーザ名を使用することとする。

【０１９７】なお、この原本性保証電子保存装置１００は、内部記録媒体１０４のアカウント管理テーブルにあらかじめアカウント名とパスワードを記憶しており、外部システムがアクセスする場合には、外部システム用のアカウント名を使用し、原本の移動やコピーをするために他の原本性保証電子保存装置にログインする際には、原本性保証電子保存装置用のアカウントを使用することとする。

【０１９８】図２８は、図１に示した原本性保証電子保存装置１００へのクライアントからのログイン処理手順を示すフローチャートである。同図に示すように、クライアントがアカウント名とログイン要求を送信し（ステップＳ２２０１）、原本性保証電子保存装置１００が、このアカウント名とログイン要求を受信したならば（ステップＳ２２０２）、内部記録媒体１０４からアカウント管理テーブルを取得する（ステップＳ２２０３）。

【０１９９】そして、クライアントがアカウント名とパスワードを送信すると（ステップＳ２２０４）、原本性保証電子保存装置１００では、アカウント管理テーブルから該当するパスワードを取得し（ステップＳ２２０５）、該当するパスワードが存在しない場合には（ステップＳ２２０６肯定）、エラー処理をおこなって処理を終了する（ステップＳ２２０７）。

【０２００】これに対して該当するパスワードが存在する場合には（ステップＳ２２０６否定）、乱数を生成してクライアントに送信する（ステップＳ２２０８～Ｓ２２０９）とともに、乱数とパスワードを合わせたものに対してハッシュ値を計算する（ステップＳ２２１０）。

40

【０２０１】一方、クライアントがこの乱数を受信したならば（ステップＳ２２１１）、乱数とパスワードを合わせたものに対してハッシュ値を計算し（ステップＳ２２１２）、計算したハッシュ値を送信する（ステップＳ２２１３）。

【０２０２】そして、原本性保証電子保存装置１００が、このハッシュ値を受信したならば（ステップＳ２２１４）、両ハッシュ値を比較して両者が一致する場合には（ステップＳ２２１５肯定）、成功した終了コードを送信し（ステップＳ２２１６）、両者が一致しない場合には（ステップＳ２２１５否定）、エラー処理をおこなう（ステップＳ２２１８）。その後、クライアントがこの終了コードを受信（ステップＳ２２１７）したならば、代理ユーザ名を送信して（ステップＳ２２１９）ログイン処理を終了する。

【０２０３】そして、原本性保証電子保存装置１００が、この代理ユーザ名を受信したならば（ステップＳ２２２０）、受け取った代理ユーザ名をアクセスユーザ名として内部に保持して（ステップＳ２２２１）処理を終了する。なお、ステップＳ２２０７およびＳ２２１８のエラー処理時には、エラーを示す旨の終了コードをクライアントに送信する。

【０２０４】次に、図１に示した原本性保証電子保存装置１００による日時の管理について説明する。この原本性保証電子保存装置１００では、データアクセス履歴などに記録する日時は装置内部のタイマ１０５から取得するが、このタイマ１０５は設定変更が可能であるため、タイマ１０５を不正に変更することによりデータアクセス日時を偽ることが可能となる。

【０２０５】このため、本実施の形態では、タイマ１０５の設定をおこなうと図２９（ａ）に示すように、タイマ設定履歴を自動的に内部記憶媒体１０４に記憶するよう構成している。

【０２０６】ここで、タイマＩＤは、装置内部で自動的に付与されるシーケンシャルな番号であり、タイマの設定を変更する都度番号が増える。また、データアクセス履歴に含まれる日時情報にはタイマＩＤも含まれる。

【０２０７】同図に示す場合に、タイマＩＤ＝３において不正に日付を１月ずらし、その後タイマＩＤ＝４で日付を戻していることが分かるため、データアクセス履歴の日時にタイマＩＤ＝３の履歴が付されているデータは、不正に日時を偽ろうとした可能性があることが判明する。なお、タイマ設定履歴は原本性保証電子保存装置１００の内部記憶媒体１０４に記録する。

【０２０８】また、原本性保証電子保存装置１００から他の原本性保証電子保存装置へデータを移動したりコピ

41

ーする場合にも、データアクセス履歴の日時に不都合が生じないようにするために、図２９（ｂ）に示すデータアクセス履歴をデータ属性情報に取り込む。なお、このデータアクセス履歴は、データ属性情報ファイルに記憶する。

【０２０９】具体的には、同図に示す例では、移動先の原本性保証電子保存装置R010-0001055の日時19990217 10:13:43 ＩＤ＝２が、移動元の原本性保証電子保存装置R010-0001032の日時19990217 10:10:21 ＩＤ＝３に相当することが分かるため、移動したデータに不正が見つかった場合には、原本性保証電子保存装置をまたいで履歴を辿ることができる。

【０２１０】次に、図１に示した原本性保証電子保存装置１００が用いる保存データリストファイル、データ属性情報ファイル、バージョン属性情報、コンテンツ属性情報、媒体認証コードリスト、アカウント管理リスト、日時情報およびタイマ設定履歴ファイルの一例について図３０～図３２を用いて説明する。

【０２１１】図３０（ａ）は、原本性保証電子保存装置１００が用いる保存データリストファイルの一例を示す図であり、同図に示すように、この保存データリストファイルは、メッセージ認証子（リストＭＡＣ）と各リストエントリからなる。なお、ここで言う原本化とは、属性コードを「仮原本」から「原本」に変更することを意味する。そして、最初のリストＭＡＣを除いた部分が改ざん検知読み出し処理した際の保存データリストとなる。

【０２１２】なお、媒体識別番号は、原本性保証電子保存装置の識別番号（たとえば、R01093）に媒体をフォーマットした順に振るシーケンシャルな番号（たとえば、0012）をつけたもの（たとえば、R01093-0012）とする。

【０２１３】媒体識別番号ファイルは、媒体識別番号を内容として含む規定のファイル名（たとえば、medium.id）のファイルとして保存する。また、保存データリストファイルは、媒体識別番号（たとえば、R01093-0012）の後ろに.listを付加したファイル名（たとえば、R01093-0012.list）で保存する。

【０２１４】図３０（ｂ）は、原本性保証電子保存装置１００が用いるデータ属性情報ファイルの一例を示す図であり、同図に示すように、このデータ属性情報ファイルは、メッセージ認証子（リストＭＡＣ）、属性管理データ、簡易バージョン属性情報およびアクセス履歴からなる。

【０２１５】そして、最初のデータ属性ＭＡＣを除いた部分が改ざん検知読み出し処理した際のデータ属性情報となる。また、データ識別番号は、原本性保証電子保存装置識別番号（たとえば、R01093）と、最新データ識別番号から得られる番号（たとえば、00123210）とをつなげたもの（R01093-00123210）となる。

42

【０２１６】また、データ識別情報ファイルは、そのデータ識別番号に.datをつけたファイル名（たとえば、R01093-00123210.dat）で保存する。また、謄本データの場合には、複製した元の原本データのデータ識別番号を参照原本識別番号として記録する。謄本データは、データ識別番号の前にC-を付け、C-R01093-00123210のようにする。

【０２１７】図３１（ａ）は、原本性保証電子保存装置１００が用いるバージョン属性情報の一例を示す図であり、同図に示すように、このバージョン属性情報は、メッセージ認証子（リストＭＡＣ）と、バージョン管理データとからなる。

【０２１８】バージョン属性情報ファイルは、そのバージョン番号に応じてデータ識別番号にバージョン番号を付けたものに.datをつけたファイル名（たとえば、ver.7ならR01093-00123210-7.dat）で保存する。最初のバージョン属性ＭＡＣを除いた部分が改ざん検知読み出し処理した際のバージョン属性情報となる。

【０２１９】図３１（ｂ）は、原本性保証電子保存装置１００が用いるコンテンツ属性情報の一例を示す図であり、同図に示すように、このコンテンツ属性情報は、メッセージ認証子（コンテンツ属性ＭＡＣ）とコンテンツ管理データからなる。

【０２２０】前のバージョンから更新されていないコンテンツは、前バージョンのコンテンツのデータファイルを兼用するため、現バージョンにおけるデータファイルが存在しないが、存在するものとしてコンテンツ管理データ内のデータファイル名を記録する。

【０２２１】図３１（ｃ）は、原本性保証電子保存装置１００が用いる媒体認証リストコードの一例を示す図であり、同図に示すように、この媒体認証リストコードは、媒体識別番号およびメッセージ認証子（リストＭＡＣ）からなる複数の認証コードエントリにより形成される。

【０２２２】図３２（ａ）は、原本性保証電子保存装置１００が用いるアカウント管理リストの一例を示す図であり、同図に示すように、このアカウント管理リストは、アカウント名およびパスワードからなる各アカウントエントリからなる。なお、このアカウント管理リストは、任意の数のアカウントが登録できるような構造としているが、最初から存在するクライアント用のアカウントや、原本性保証電子保存装置用のアカウントについては図示省略している。

【０２２３】図３２（ｂ）は、原本性保証電子保存装置１００が用いる日時情報の内容を示す図であり、同図に示すように、この日時情報は、「年」、「月」、「日」、「時」、「分」、「秒」、「ＧＳＴ（世界標準時）からのずれ」および「タイマＩＤ」からなる。

【０２２４】図３２（ｃ）は、原本性保証電子保存装置１００が用いるタイマ設定履歴ファイルの内容を示す図

であり、同図に示すように、このタイマ設定履歴ファイルは、設定前の日時情報、設定後の日時情報およびアカウント名からなる各タイマ設定履歴からなる。

【０２２５】

【発明の効果】以上説明したように、請求項１の発明によれば、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうよう構成したので、複数のファイルから形成される複合文書の原本性を効率良く保証することができる原本性保証電子保存装置が得られるという効果を奏する。

【０２２６】また、請求項２の発明によれば、電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに記憶部に保存するよう構成したので、効率良く改ざん検知をおこなうことができる原本性保証電子保存装置が得られるという効果を奏する。

【０２２７】また、請求項３の発明によれば、電子データに対応する第１の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を属性情報とともに記憶部に保存するよう構成したので、電子データ並びにアクセス履歴を含む改ざんを効率良く検知することができる原本性保証電子保存装置が得られるという効果を奏する。

【０２２８】また、請求項４の発明によれば、複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定し、算定した第１の改ざん検知情報を含む版管理情報を作成して第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を算定し、算定した第３の改ざん検知情報を含むデータエントリを作成して記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第４の改ざん検知情報を算定し、算定した第４の改ざん検知情報と複数のコンテンツとを記憶部に格納するよう構成したので、複数のコンテンツファイルからなる新規データを改ざん防止措置を施しつつ効率良く格納することができる原本性保証電子保存装置が得られるという効果を奏する。

【０２２９】また、請求項５の発明によれば、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、記憶部から第４の改ざん検知情報およびデータリストを読み出し、読み出した第４の改ざん検知情報および復号鍵を用いてデータリストの改ざん検知をおこない、データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、このエントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第２の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および復号鍵を用いてコンテンツファイルの改ざん検知をおこない、コンテンツファイルが改ざんされていない場合に、記憶部に記憶したコンテンツファイルを要求元に提供するよう構成したので、多段階に渡って改ざんを防止しつつコンテンツファイルの読み出しを効率良くおこなうことができる原本性保証電子保存装置が得られるという効果を奏する。

【０２３０】また、請求項６の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、記憶部から第４の改ざん検知情報およびデータリストを読み出し、読み出した第４の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定し、算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を暗号鍵を用いて算定し、算定された第３の改ざん検知情報を含むデータエントリを作成し、記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第４の改ざん検知情報を算定し、算定された第４の改ざん検知情報と複数のコンテンツとを記憶部に格納するよう構成したので、電子データが複数のコンテンツファイルからなる場合であっても、バージョンアップを効率良くおこなうことができる原本性保証電子保存装置が得られるという効果を奏する。

【０２３１】また、請求項７の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、第４の改ざん検知情報およびデータリストを読み出し、読み出した第４の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、属性情報から複製対象となる版に係る第２の改ざん検知情報を取り出し、該第２の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該

第１の改ざん検知情報および復号鍵を用いて前記コンテンツファイルの改ざん検知をおこない、記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製し、複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更し、変更された属性コードを含む属性情報および暗号鍵を用いて第３の改ざん検知情報を再算定し、再算定された第３の改ざん検知情報を含むエントリによりデータリストを更新し、更新後のデータリストに係る第４の改ざん検知情報を暗号鍵を用いて再算定するよう構成したので、電子データが複数のコンテンツファイルからなる場合であっても、版を指定した複製を効率良くおこなうことができる原本性保証電子保存装置が得られるという効果を奏する。

【０２３２】また、請求項８の発明によれば、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうよう構成したので、複数のファイルから形成される複合文書の原本性を効率良く保証することができる原本性保証電子保存方法が得られるという効果を奏する。

【０２３３】また、請求項９の発明によれば、電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに記憶部に保存するよう構成したので、効率良く改ざん検知をおこなうことができる原本性保証電子保存方法が得られるという効果を奏する。

【０２３４】また、請求項１０の発明によれば、電子データに対応する第１の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を属性情報とともに記憶部に保存するよう構成したので、電子データ並びにアクセス履歴を含む改ざんを効率良く検知することができる原本性保証電子保存方法が得られるという効果を奏する。

【０２３５】また、請求項１１の発明によれば、複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定し、算定した第１の改ざん検知情報を含む版管理情報を作成して第２の改ざん検知情報を算定し、算定した第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を算定し、算定した第３の改ざん検知情報を含むデータエントリを作成して記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第４の改ざん検知情報を算定し、算定した第４の改ざん検知情報と複数のコンテンツとを記憶部に格納するよう構成したので、複数のコンテンツファイルからなる新規データを改ざん防止措置を施しつつ効率良く格納することができる原本性保証電子保存方法が得られるという効果を奏する。

【０２３６】また、請求項１２の発明によれば、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、記憶部から第４の改ざん検知情報およびデータリストを読み出し、読み出した第４の改ざん検知情報および復号鍵を用いてデータリストの改ざん検知をおこない、データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、このエントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第２の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および復号鍵を用いてコンテンツファイルの改ざん検知をおこない、コンテンツファイルが改ざんされていない場合に、記憶部に記憶したコンテンツファイルを要求元に提供するよう構成したので、多段階に渡って改ざんを防止しつつコンテンツファイルの読み出しを効率良くおこなうことができる原本性保証電子保存方法が得られるという効果を奏する。

【０２３７】また、請求項１３の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、記憶部から第４の改ざん検知情報およびデータリストを読み出し、読み出した第４の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第１の改ざん検知情報をそれぞれ算定し、算定された第２の改ざん検知情報を含む属性情報に係る第３の改ざん検知情報を暗号鍵を用いて算定し、算定された第３の改ざん検知情報を含むデータエントリを作成し、記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第４の改ざん検知情報を算定し、算定された第４の改ざん検知情報と複数のコンテンツとを記憶部に格納するよう構成したので、電子データが複数のコンテンツファイルからなる場合であっても、バージョンアップを効率良くおこなうことができる原本性保証電子保存方法が得られるという効果を奏する。

【０２３８】また、請求項１４の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、第４の改ざん検知情報およびデータリスト

を読み出し、読み出した第４の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第３の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、属性情報から複製対象となる版に係る第２の改ざん検知情報を取り出し、該第２の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第１の改ざん検知情報を取り出し、該第１の改ざん検知情報および復号鍵を用いて前記コンテンツファイルの改ざん検知をおこない、記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製し、複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更し、変更された属性コードを含む属性情報および暗号鍵を用いて第３の改ざん検知情報を再算定し、再算定された第３の改ざん検知情報を含むエントリによりデータリストを更新し、更新後のデータリストに係る第４の改ざん検知情報を暗号鍵を用いて再算定するよう構成したので、電子データが複数のコンテンツファイルからなる場合であっても、版を指定した複製を効率良くおこなうことができる原本性保証電子保存方法が得られるという効果を奏する。

【０２３９】また、請求項１５の発明に係る記録媒体は、請求項８～１４のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項８～１４の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図１】この実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。

【図２】図１に示した大容量記憶媒体に保存する保存データのデータ構造の一例を示す説明図である。

【図３】図１に示した原本性保証電子保存装置による新規データの保存処理手順を示すフローチャートである。

【図４】図３に示したバージョン属性情報の作成処理手順を示すフローチャートである。

【図５】図４に示したコンテンツ属性情報の作成処理手順を示すフローチャートである。

【図６】図３に示したデータ属性情報の作成処理手順を示すフローチャートである。

【図７】図３に示した保存データリストエントリの追加処理手順を示すフローチャートである。

【図８】図３～図７において説明した新規データの保存処理の一例を示す説明図である。

【図９】図１に示した大容量記憶媒体のマウント処理手順を示すフローチャートである。

【図１０】図１に示した原本性保証電子保存装置によるデータ読み出し処理手順を示すフローチャート（その１）である。

【図１１】図１に示した原本性保証電子保存装置によるデータ読み出し処理手順を示すフローチャート（その２）である。

【図１２】図１に示した原本性保証電子保存装置による謄本作成処理手順を示すフローチャート（その１）である。

【図１３】図１に示した原本性保証電子保存装置による謄本作成処理手順を示すフローチャート（その２）である。

【図１４】図１に示した原本性保証電子保存装置による謄本作成処理手順を示すフローチャート（その３）である。

【図１５】図１に示した原本性保証電子保存装置による謄本作成処理手順を示すフローチャート（その４）である。

【図１６】図１に示した原本性保証電子保存装置のデータ移動処理手順を示すフローチャート（その１）である。

【図１７】図１に示した原本性保証電子保存装置のデータ移動処理手順を示すフローチャート（その２）である。

【図１８】図１３に示した保存データリストエントリの削除処理手順を示すフローチャートである。

【図１９】異なる原本性保証電子保存装置にデータ移動処理をおこなう場合の移動先の原本性保証電子保存装置における転送受け入れ処理手順を示すフローチャート（その１）である。

【図２０】異なる原本性保証電子保存装置にデータ移動処理をおこなう場合の移動先の原本性保証電子保存装置における転送受け入れ処理手順を示すフローチャート（その２）である。

【図２１】図１に示した原本性保証電子保存装置によるデータの削除処理手順を示すフローチャートである。

【図２２】図１に示した原本性保証電子保存装置によるデータ属性コードの変更態様を示す説明図である。

【図２３】図１に示した原本性保証電子保存装置によるデータ属性コードの変更処理手順を示すフローチャート（その１）である。

【図２４】図１に示した原本性保証電子保存装置によるデータ属性コードの変更処理手順を示すフローチャート（その２）である。

【図２５】図２４に示した保存データリストエントリの更新処理手順を示すフローチャートである。

【図２６】図１に示した原本性保証電子保存装置によるデータのバージョンアップ処理手順を示すフローチャートである。

【図２７】図１に示した原本性保証電子保存装置によるデータの編集処理手順を示すフローチャートである。

49

【図２８】図１に示した原本性保証電子保存装置へのクライアントからのログイン処理手順を示すフローチャートである。

【図２９】図１に示した原本性保証電子保存装置が用いるタイマ設定履歴およびアクセス履歴の一例を示す図である。

【図３０】図１に示した原本性保証電子保存装置が用いる保存データリストファイルおよびデータ属性情報ファイルの一例を示す図である。

【図３１】図１に示した原本性保証電子保存装置が用いるバージョン属性情報、コンテンツ属性情報および媒体認証リストコードの一例を示す図である。

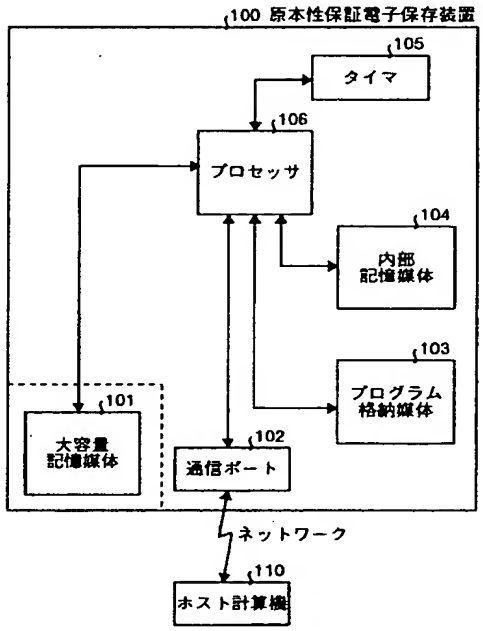
50

【図３２】図１に示した原本性保証電子保存装置が用いるアカウント管リスト、日時情報およびタイマ設定履歴ファイルの一例を示す説明図である。

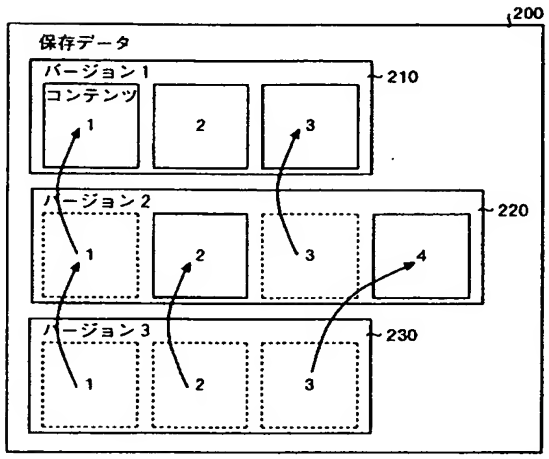
【符号の説明】

１００　原本性保証電子保存装置
１０１　大容量記憶媒体
１０２　通信ポート
１０３　プログラム格納媒体
１０４　内部記録媒体
１０５　タイマ
１０６　プロセッサ
１１０　ホスト計算機

【図１】



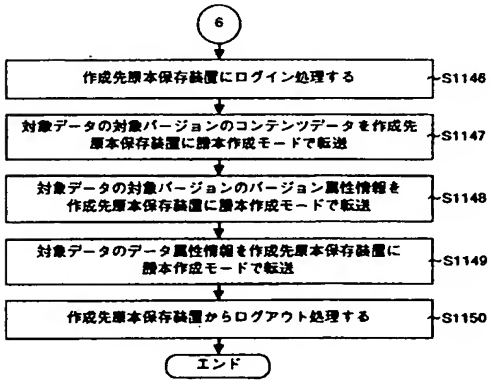
【図２】



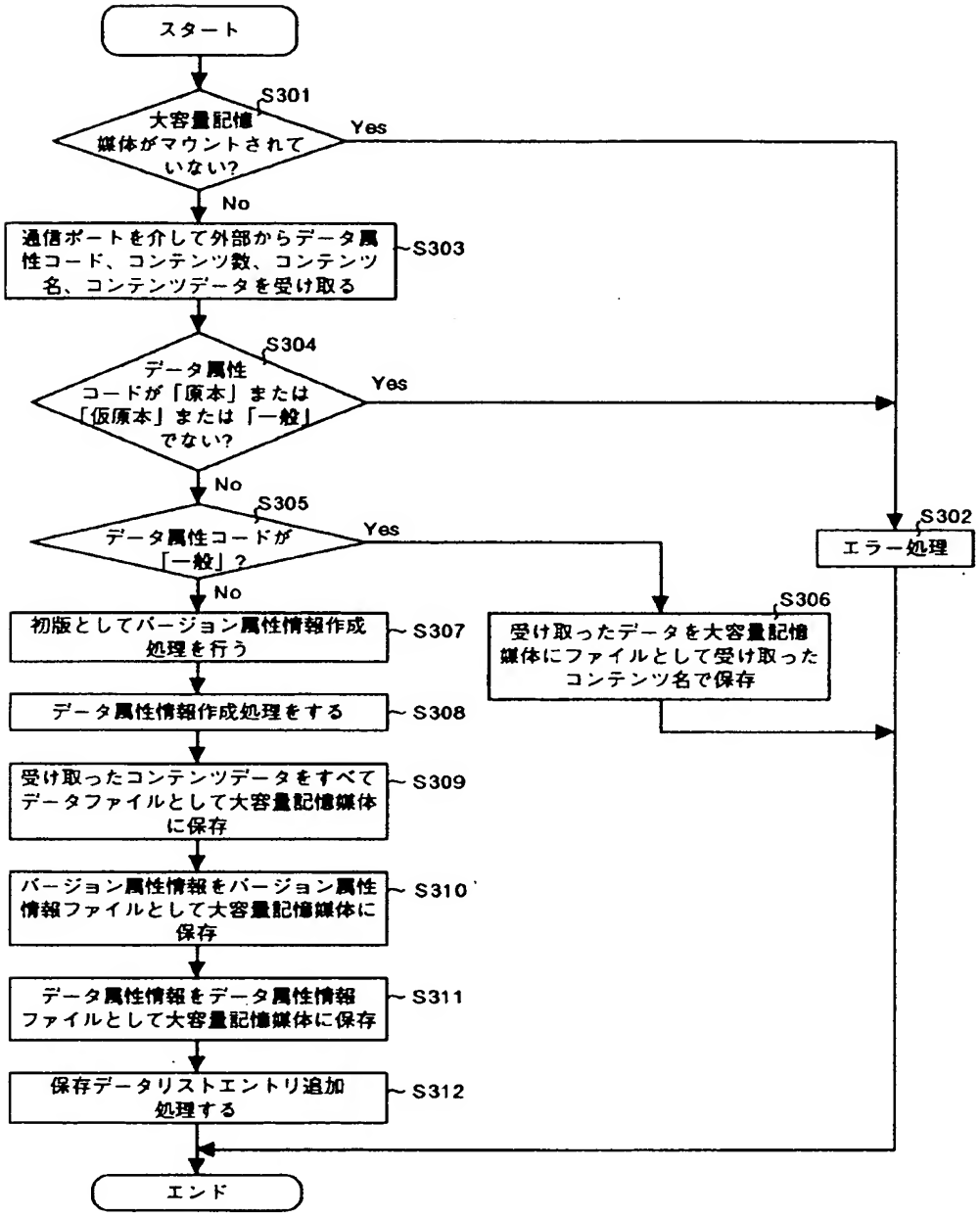
【図２２】

復旧前	復旧後
謄本	原本
バックアップ仮原本	仮原本
バックアップ原本	原本
バックアップ謄本	謄本

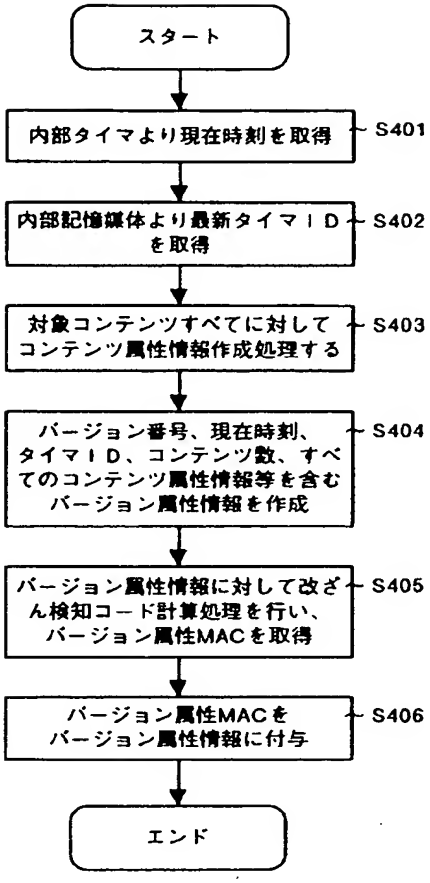
【図１５】



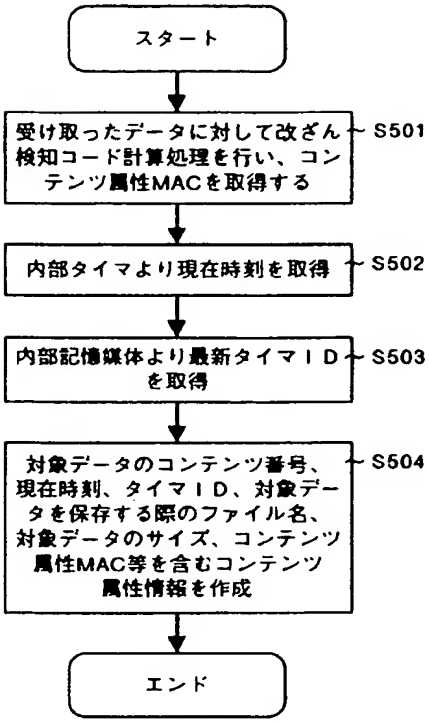
【図３】


スタート
S301
大容量記憶媒体がマウントされていない?
Yes
No
通信ポートを介して外部からデータ属性コード、コンテンツ数、コンテンツ名、コンテンツデータを受け取る
S303
S304
データ属性コードが「原本」または「仮原本」または「一般」でない?
Yes
No
S305
データ属性コードが「一般」?
Yes
No
S302
エラー処理
S306
受け取ったデータを大容量記憶媒体にファイルとして受け取ったコンテンツ名で保存
初版としてバージョン属性情報作成処理を行う
S307
データ属性情報作成処理をする
S308
受け取ったコンテンツデータをすべてデータファイルとして大容量記憶媒体に保存
S309
バージョン属性情報をバージョン属性情報ファイルとして大容量記憶媒体に保存
S310
データ属性情報をデータ属性情報ファイルとして大容量記憶媒体に保存
S311
保存データリストエントリ追加処理する
S312
エンド

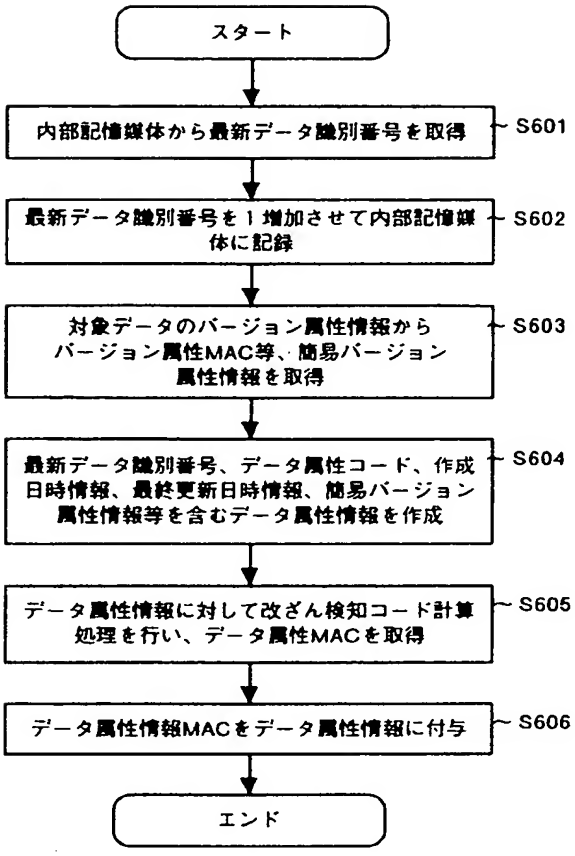
【図４】


スタート
内部タイマより現在時刻を取得
S401
内部記憶媒体より最新タイマＩＤを取得
S402
対象コンテンツすべてに対してコンテンツ属性情報作成処理する
S403
バージョン番号、現在時刻、タイマＩＤ、コンテンツ数、すべてのコンテンツ属性情報等を含むバージョン属性情報を作成
S404
バージョン属性情報に対して改ざん検知コード計算処理を行い、バージョン属性MACを取得
S405
バージョン属性MACをバージョン属性情報に付与
S406
エンド

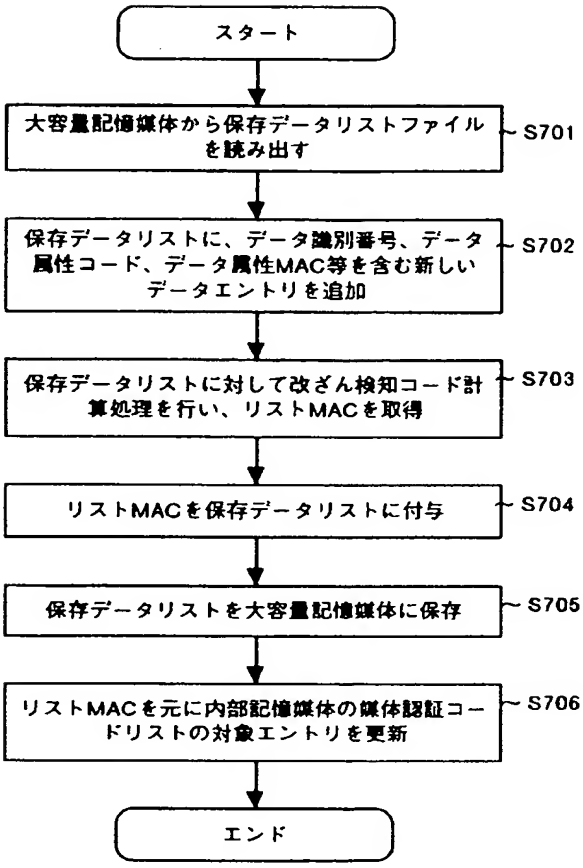
【図５】


スタート
受け取ったデータに対して改ざん検知コード計算処理を行い、コンテンツ属性MACを取得する
S501
内部タイマより現在時刻を取得
S502
内部記憶媒体より最新タイマＩＤを取得
S503
対象データのコンテンツ番号、現在時刻、タイマＩＤ、対象データを保存する際のファイル名、対象データのサイズ、コンテンツ属性MAC等を含むコンテンツ属性情報を作成
S504
エンド

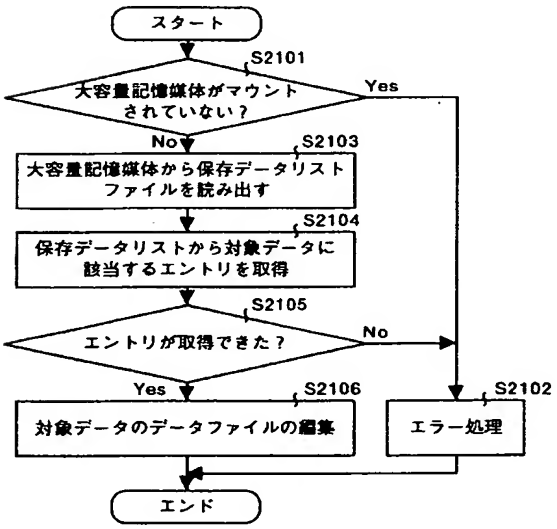
【図６】


スタート
内部記憶媒体から最新データ識別番号を取得
S601
最新データ識別番号を１増加させて内部記憶媒体に記録
S602
対象データのバージョン属性情報からバージョン属性MAC等、簡易バージョン属性情報を取得
S603
最新データ識別番号、データ属性コード、作成日時情報、最終更新日時情報、簡易バージョン属性情報等を含むデータ属性情報を作成
S604
データ属性情報に対して改ざん検知コード計算処理を行い、データ属性MACを取得
S605
データ属性情報MACをデータ属性情報に付与
S606
エンド

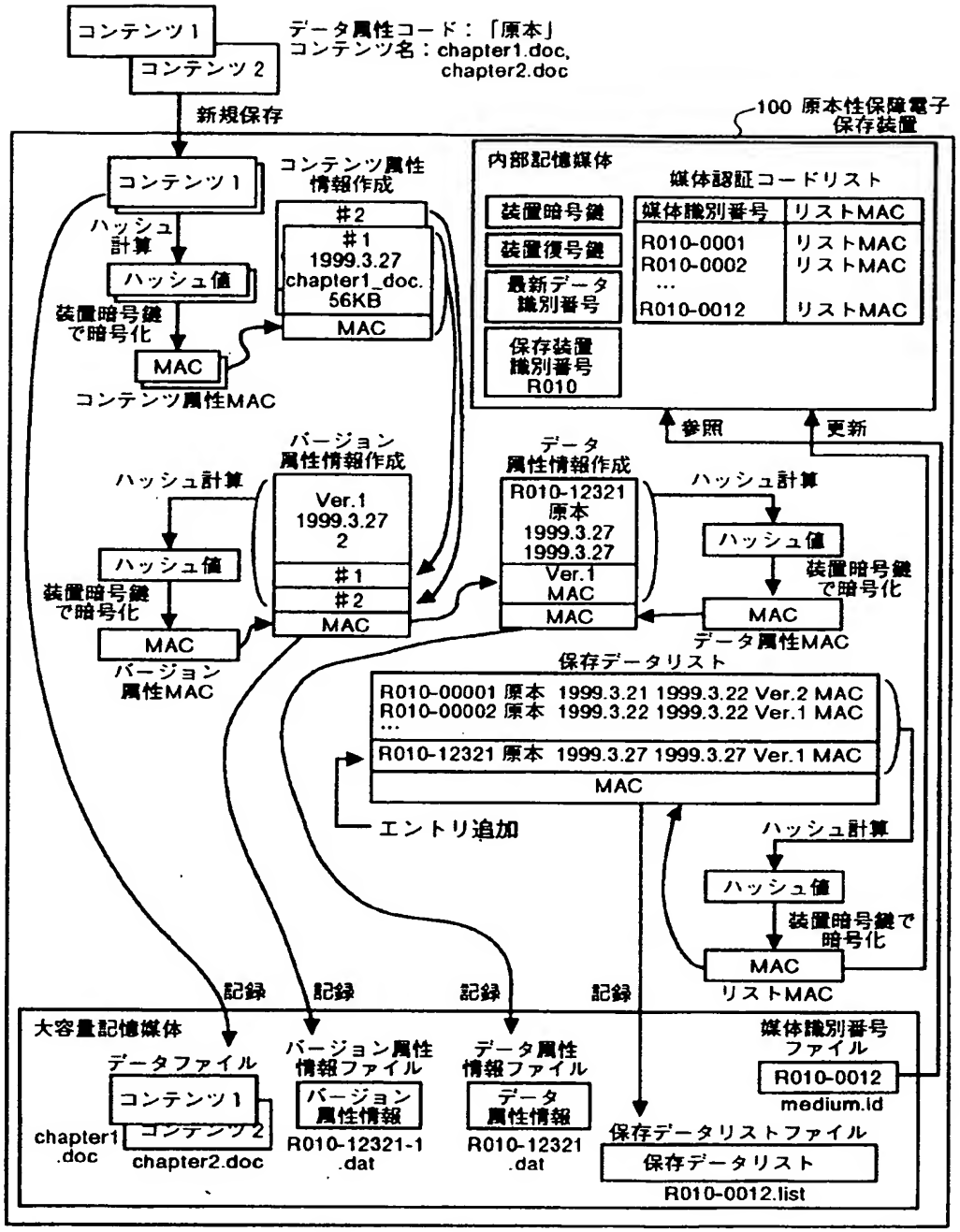
【図７】


スタート
大容量記憶媒体から保存データリストファイルを読み出す
S701
保存データリストに、データ識別番号、データ属性コード、データ属性MAC等を含む新しいデータエントリを追加
S702
保存データリストに対して改ざん検知コード計算処理を行い、リストMACを取得
S703
リストMACを保存データリストに付与
S704
保存データリストを大容量記憶媒体に保存
S705
リストMACを元に内部記憶媒体の媒体認証コードリストの対象エントリを更新
S706
エンド

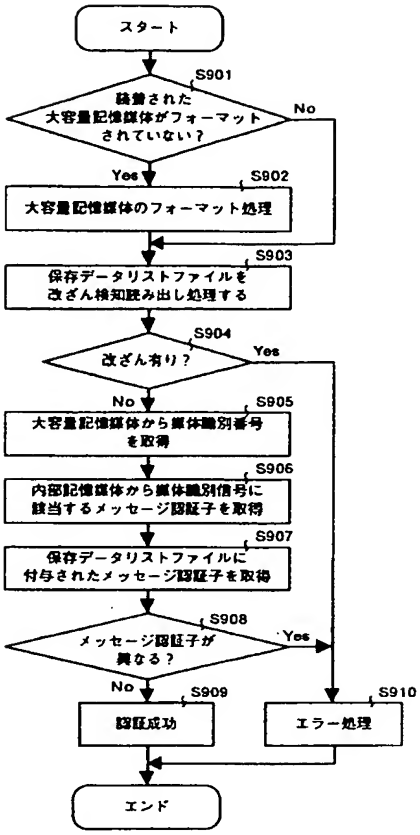
【図２７】


スタート
S2101
大容量記憶媒体がマウントされていない？
Yes
No
S2103
大容量記憶媒体から保存データリストファイルを読み出す
S2104
保存データリストから対象データに該当するエントリを取得
S2105
エントリが取得できた？
No
Yes
S2106
対象データのデータファイルの編集
S2102
エラー処理
エンド

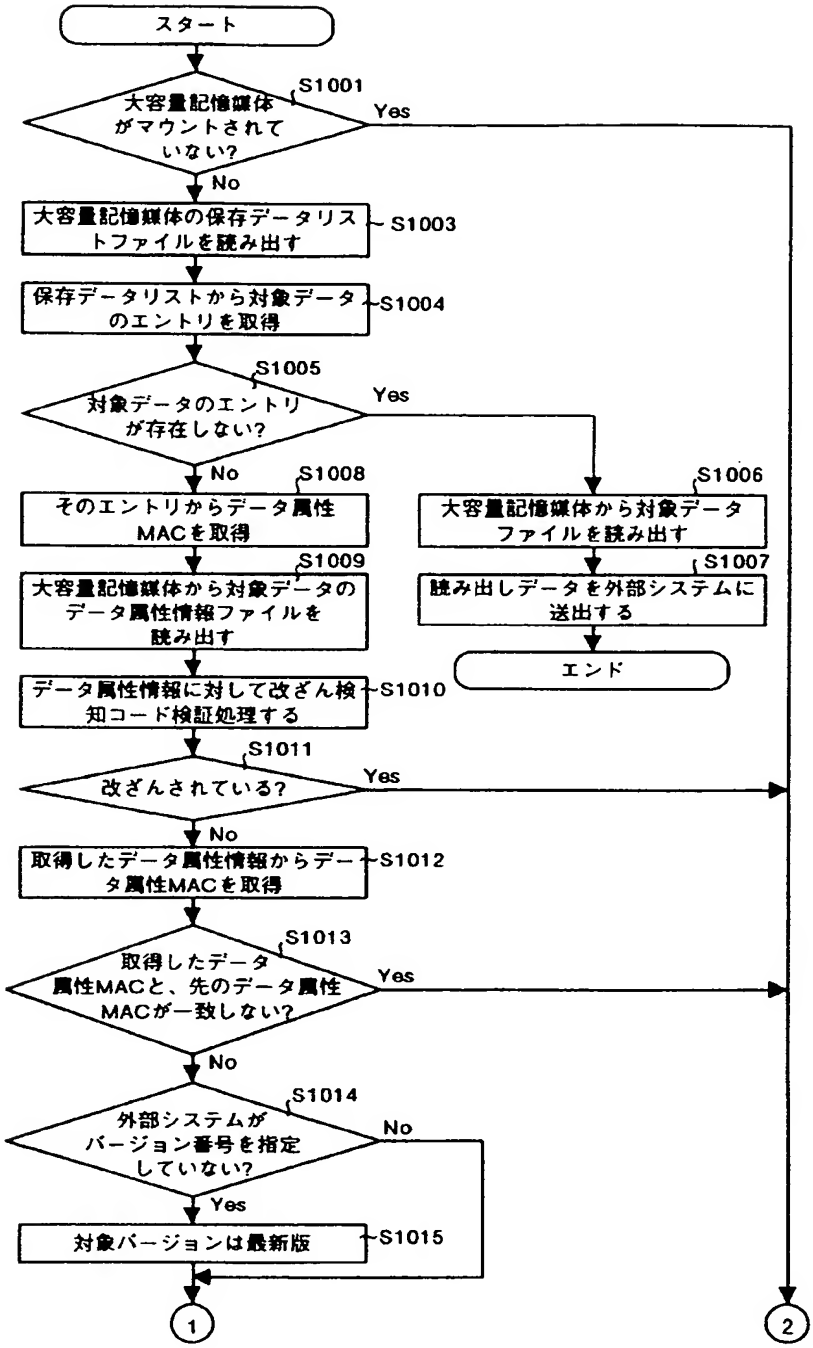
【図８】


コンテンツ１
コンテンツ２
データ属性コード：「原本」
コンテンツ名：chapter1.doc,
chapter2.doc
新規保存
100 原本性保障電子保存装置
コンテンツ１
コンテンツ属性情報作成
ハッシュ計算
ハッシュ値
装置暗号鍵で暗号化
MAC
コンテンツ属性MAC
#2
#1
1999.3.27
chapter1_doc.
56KB
MAC
内部記憶媒体
装置暗号鍵
装置復号鍵
最新データ識別番号
保存装置識別番号
R010
媒体認証コードリスト
媒体識別番号
リストMAC
R010-0001
R010-0002
…
R010-0012
参照
更新
バージョン属性情報作成
Ver.1
1999.3.27
2
#1
#2
MAC
ハッシュ計算
ハッシュ値
装置暗号鍵で暗号化
MAC
バージョン属性MAC
データ属性情報作成
R010-12321
原本
1999.3.27
1999.3.27
Ver.1
MAC
MAC
ハッシュ計算
ハッシュ値
装置暗号鍵で暗号化
MAC
データ属性MAC
保存データリスト
R010-00001 原本 1999.3.21 1999.3.22 Ver.2 MAC
R010-00002 原本 1999.3.22 1999.3.22 Ver.1 MAC
…
R010-12321 原本 1999.3.27 1999.3.27 Ver.1 MAC
MAC
エントリ追加
ハッシュ計算
ハッシュ値
装置暗号鍵で暗号化
MAC
リストMAC
記録
記録
記録
記録
大容量記憶媒体
データファイル
コンテンツ１
コンテンツ２
chapter1.doc
chapter2.doc
バージョン属性情報ファイル
バージョン属性情報
R010-12321-1.dat
データ属性情報ファイル
データ属性情報
R010-12321.dat
媒体識別番号ファイル
R010-0012
medium.id
保存データリストファイル
保存データリスト
R010-0012.list

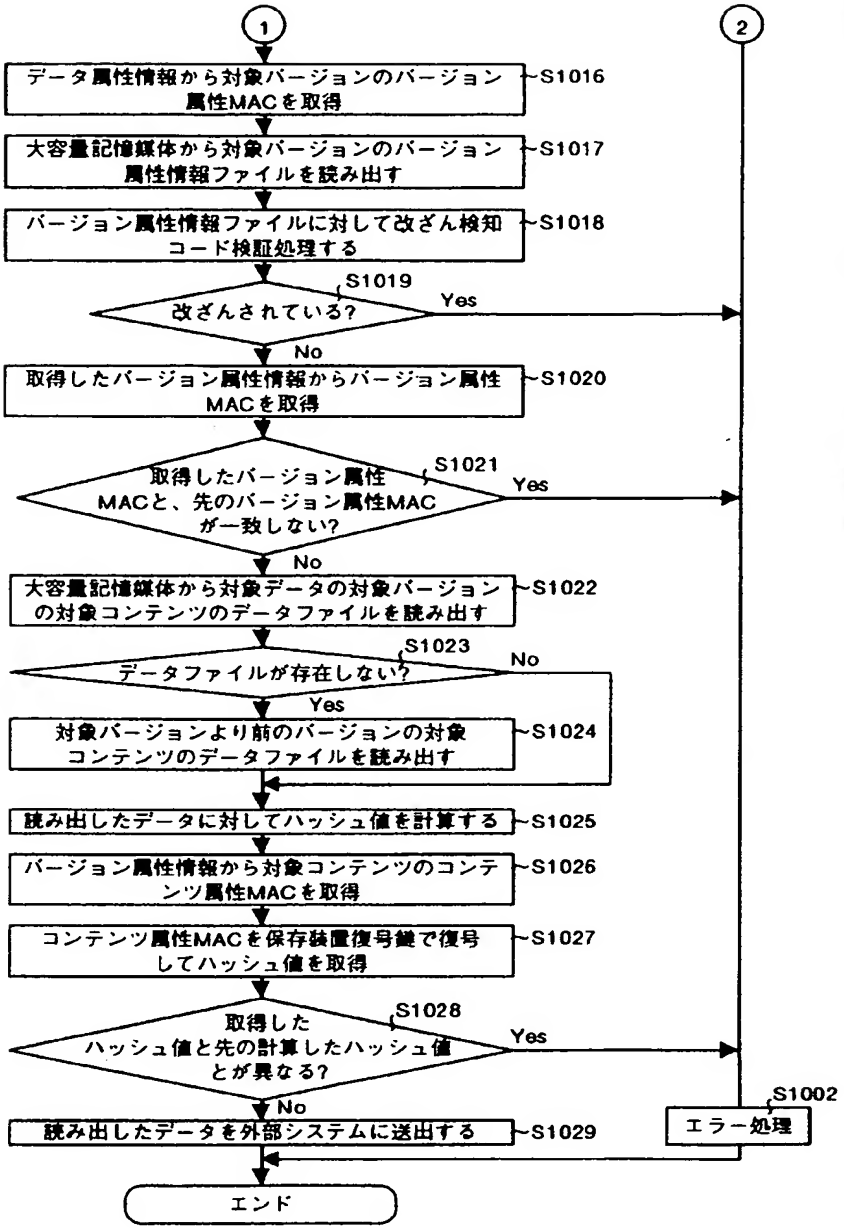
【図９】


スタート
S901
装着された大容量記憶媒体がフォーマットされていない？
No
Yes
S902
大容量記憶媒体のフォーマット処理
S903
保存データリストファイルを改ざん検知読み出し処理する
S904
改ざん有り？
Yes
No
S905
大容量記憶媒体から媒体識別番号を取得
S906
内部記憶媒体から媒体識別信号に該当するメッセージ認証子を取得
S907
保存データリストファイルに付与されたメッセージ認証子を取得
S908
メッセージ認証子が異なる？
Yes
No
S909
認証成功
S910
エラー処理
エンド

【図１０】


スタート
S1001
大容量記憶媒体がマウントされていない?
Yes
No
S1003
大容量記憶媒体の保存データリストファイルを読み出す
S1004
保存データリストから対象データのエントリを取得
S1005
対象データのエントリが存在しない?
Yes
No
S1008
そのエントリからデータ属性MACを取得
S1009
大容量記憶媒体から対象データのデータ属性情報ファイルを読み出す
S1010
データ属性情報に対して改ざん検知コード検証処理する
S1011
改ざんされている?
Yes
No
S1012
取得したデータ属性情報からデータ属性MACを取得
S1013
取得したデータ属性MACと、先のデータ属性MACが一致しない?
Yes
No
S1014
外部システムがバージョン番号を指定していない?
No
Yes
S1015
対象バージョンは最新版
S1006
大容量記憶媒体から対象データファイルを読み出す
S1007
読み出しデータを外部システムに送出する
エンド
1
2

【図１１】



【図３１】

(a)

メッセージ認証子（バージョン属性MAC）	
バージョン管理データ	バージョン番号
	バージョン作成日時情報
	コンテンツ数
	コンテンツ属性情報＃１
	コンテンツ属性情報＃２
	コンテンツ属性情報＃３
	…
	コンテンツ属性情報＃Ｎ

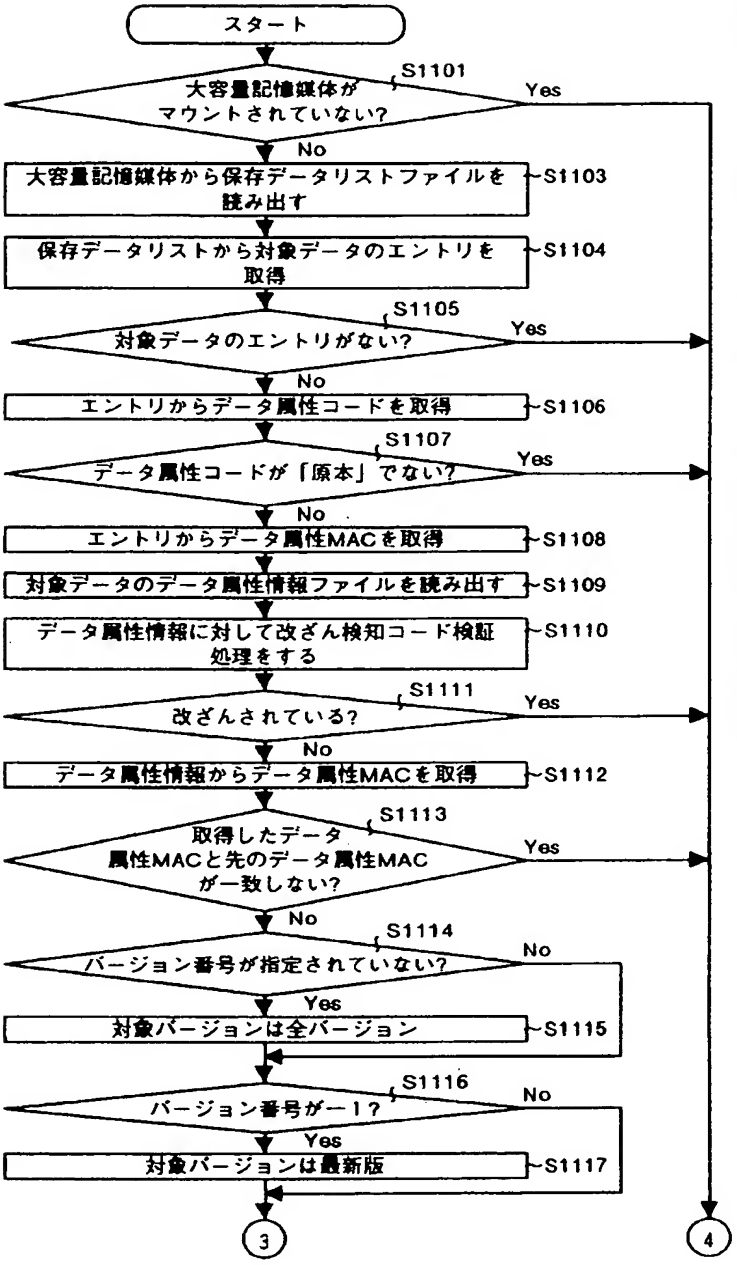
(b)

メッセージ認証子（コンテンツ属性MAC）	
コンテンツ管理データ	コンテンツ番号
	作成日時情報
	データサイズ
	データファイル名

(c)

認証コードエントリ＃１	媒体識別番号
	メッセージ認証子（リストMAC）
認証コードエントリ＃２	
認証コードエントリ＃３	
…	
認証コードエントリ＃Ｎ	

【図１２】



【図３０】

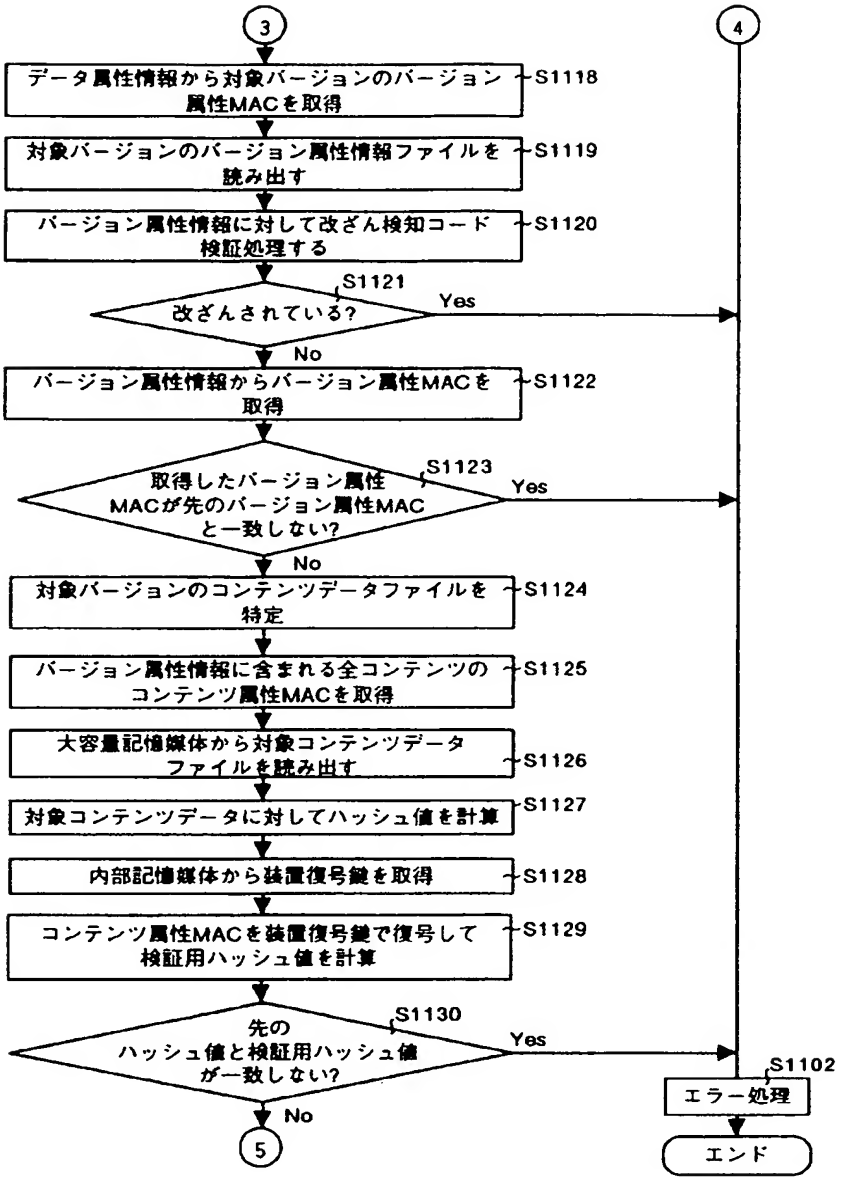
(a)

メッセージ認証子（リストMAC）	
リストエントリ＃１	データ識別番号
	属性コード
	作成日時情報
	更新日時情報
	原本化日時情報
	メッセージ認証子（データ属性MAC）
リストエントリ＃２	
リストエントリ＃３	
…	

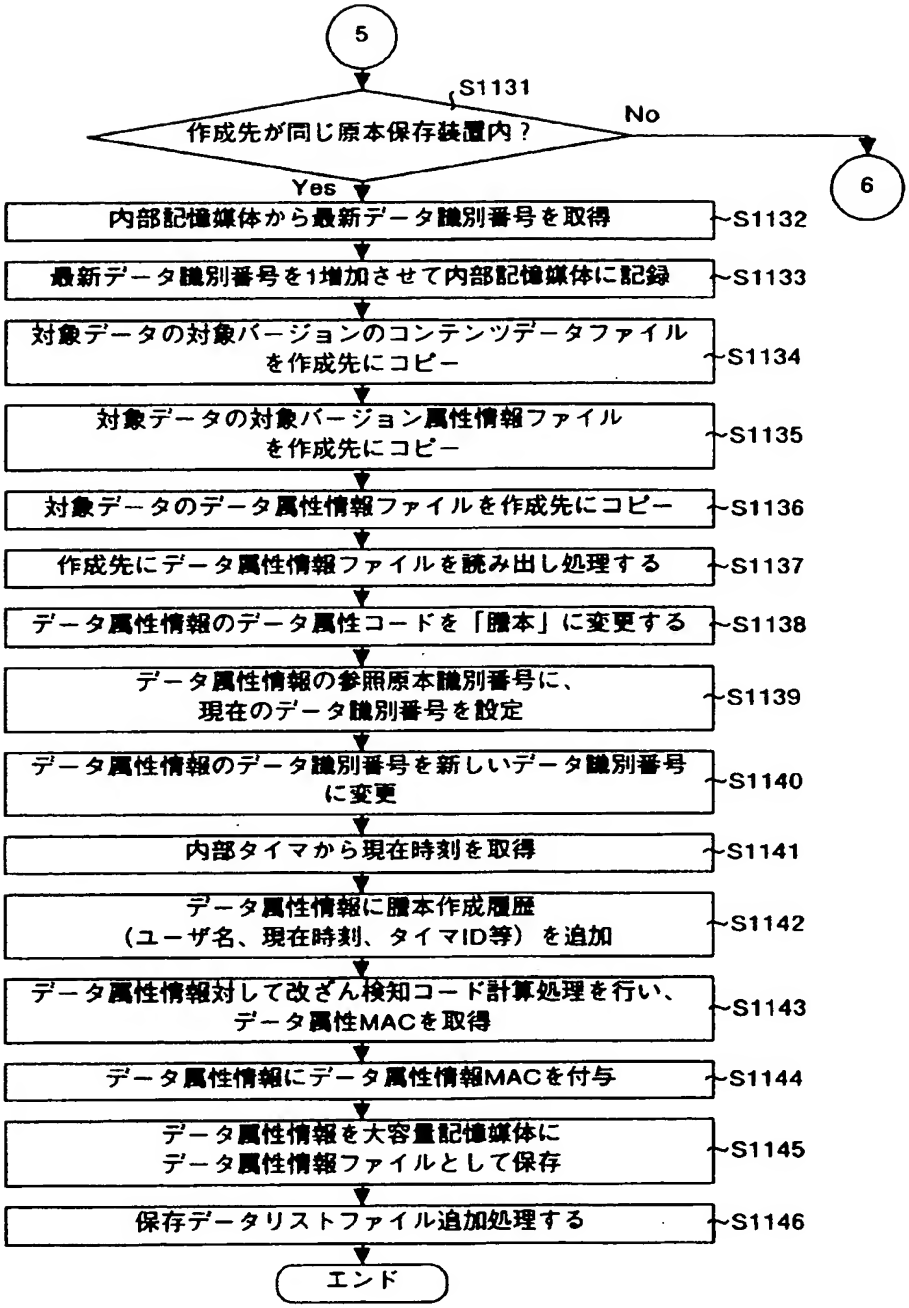
(b)

メッセージ認証子（データ属性MAC）	
属性管理データ	データ識別番号
	データ属性コード（原本、謄本、仮原本）
	参照原本識別番号
	作成日時情報
	最終更新日時情報
	最新バージョン番号
簡易バージョン属性情報＃１	メッセージ認証子（バージョン属性MAC）
	バージョン番号
	バージョン作成日時情報
	コンテンツ数
簡易バージョン属性情報＃２	
簡易バージョン属性情報＃３	
…	
簡易バージョン属性情報＃Ｎ	
アクセス履歴＃１	ユーザ名
	アクセス日時情報
	アクセス種別（作成、バージョンアップ、原本化、参照）
	保存装置識別番号
アクセス履歴＃２	
アクセス履歴＃３	
…	
アクセス履歴＃４	

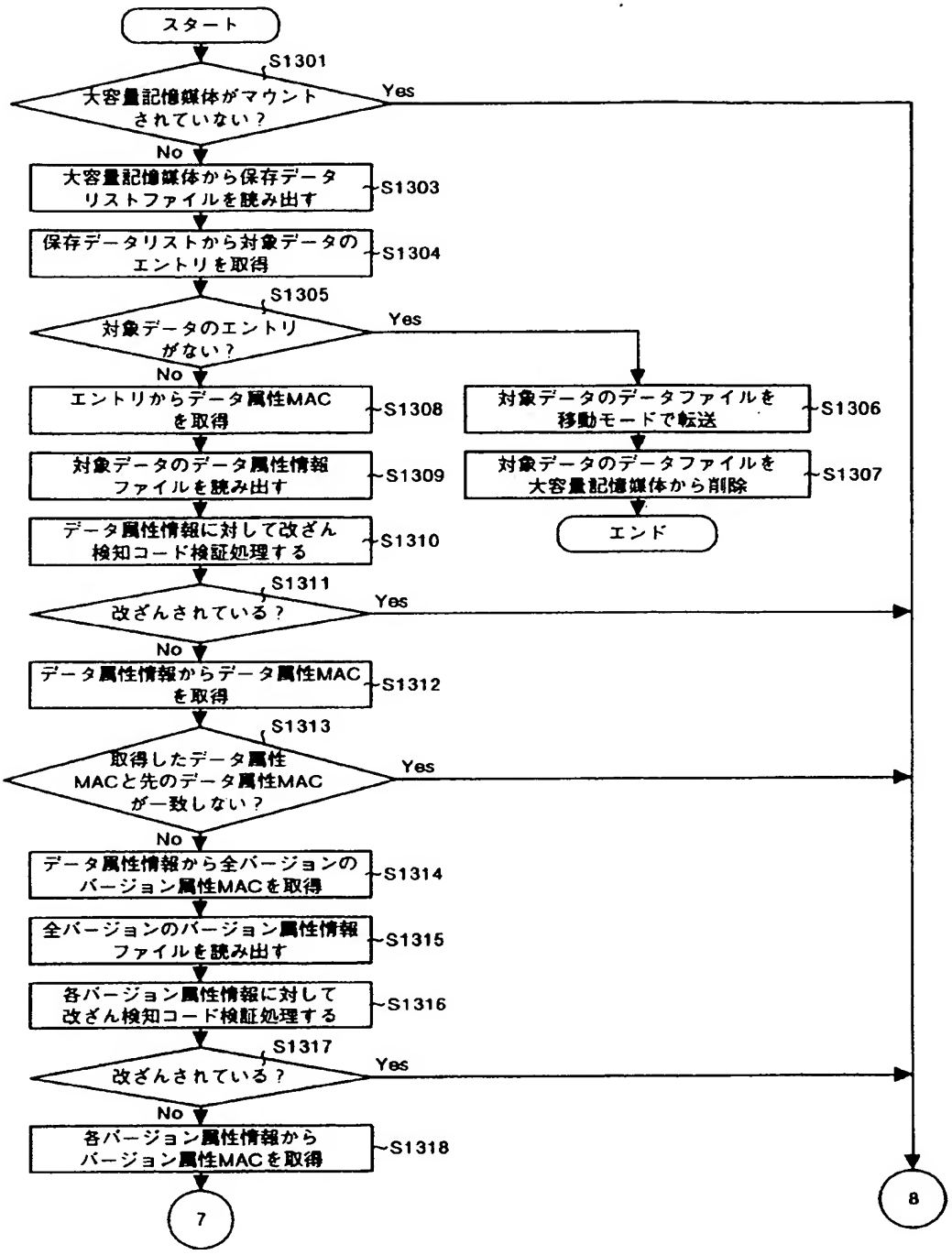
【図１３】


3
4
データ属性情報から対象バージョンのバージョン属性MACを取得
S1118
対象バージョンのバージョン属性情報ファイルを読み出す
S1119
バージョン属性情報に対して改ざん検知コード検証処理する
S1120
S1121
改ざんされている?
Yes
No
バージョン属性情報からバージョン属性MACを取得
S1122
取得したバージョン属性MACが先のバージョン属性MACと一致しない?
S1123
Yes
No
対象バージョンのコンテンツデータファイルを特定
S1124
バージョン属性情報に含まれる全コンテンツのコンテンツ属性MACを取得
S1125
大容量記憶媒体から対象コンテンツデータファイルを読み出す
S1126
対象コンテンツデータに対してハッシュ値を計算
S1127
内部記憶媒体から装置復号鍵を取得
S1128
コンテンツ属性MACを装置復号鍵で復号して検証用ハッシュ値を計算
S1129
先のハッシュ値と検証用ハッシュ値が一致しない?
S1130
Yes
No
5
S1102
エラー処理
エンド

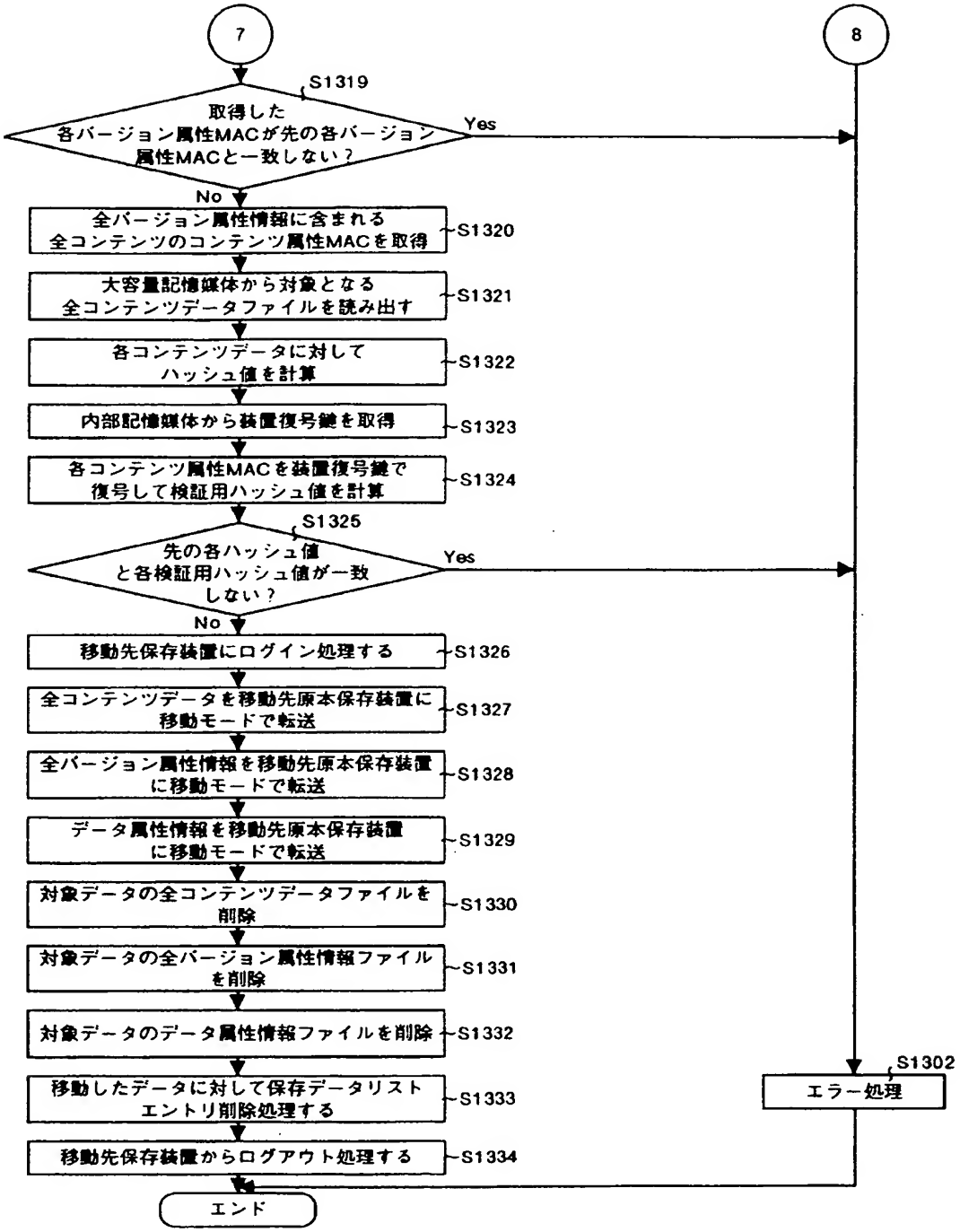
【図１４】


5
S1131
作成先が同じ原本保存装置内？
No
6
Yes
内部記憶媒体から最新データ識別番号を取得
S1132
最新データ識別番号を1増加させて内部記憶媒体に記録
S1133
対象データの対象バージョンのコンテンツデータファイルを作成先にコピー
S1134
対象データの対象バージョン属性情報ファイルを作成先にコピー
S1135
対象データのデータ属性情報ファイルを作成先にコピー
S1136
作成先にデータ属性情報ファイルを読み出し処理する
S1137
データ属性情報のデータ属性コードを「謄本」に変更する
S1138
データ属性情報の参照原本識別番号に、現在のデータ識別番号を設定
S1139
データ属性情報のデータ識別番号を新しいデータ識別番号に変更
S1140
内部タイマから現在時刻を取得
S1141
データ属性情報に謄本作成履歴（ユーザ名、現在時刻、タイマID等）を追加
S1142
データ属性情報対して改ざん検知コード計算処理を行い、データ属性MACを取得
S1143
データ属性情報にデータ属性情報MACを付与
S1144
データ属性情報を大容量記憶媒体にデータ属性情報ファイルとして保存
S1145
保存データリストファイル追加処理する
S1146
エンド

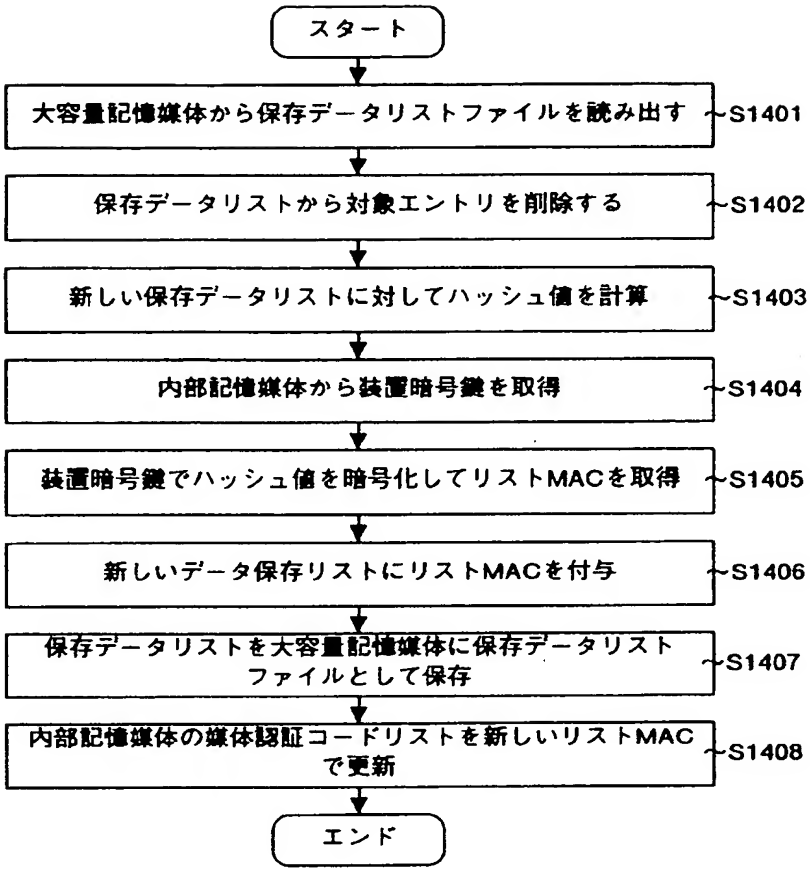
【図１６】


スタート
S1301
大容量記憶媒体がマウントされていない？
Yes
No
大容量記憶媒体から保存データリストファイルを読み出す
S1303
保存データリストから対象データのエントリを取得
S1304
S1305
対象データのエントリがない？
Yes
No
エントリからデータ属性MACを取得
S1308
対象データのデータ属性情報ファイルを読み出す
S1309
データ属性情報に対して改ざん検知コード検証処理する
S1310
対象データのデータファイルを移動モードで転送
S1306
対象データのデータファイルを大容量記憶媒体から削除
S1307
エンド
S1311
改ざんされている？
Yes
No
データ属性情報からデータ属性MACを取得
S1312
S1313
取得したデータ属性MACと先のデータ属性MACが一致しない？
Yes
No
データ属性情報から全バージョンのバージョン属性MACを取得
S1314
全バージョンのバージョン属性情報ファイルを読み出す
S1315
各バージョン属性情報に対して改ざん検知コード検証処理する
S1316
S1317
改ざんされている？
Yes
No
各バージョン属性情報からバージョン属性MACを取得
S1318
7
8

【図１７】


7
8
S1319
取得した
各バージョン属性MACが先の各バージョン
属性MACと一致しない？
Yes
No
全バージョン属性情報に含まれる
全コンテンツのコンテンツ属性MACを取得
S1320
大容量記憶媒体から対象となる
全コンテンツデータファイルを読み出す
S1321
各コンテンツデータに対して
ハッシュ値を計算
S1322
内部記憶媒体から装置復号鍵を取得
S1323
各コンテンツ属性MACを装置復号鍵で
復号して検証用ハッシュ値を計算
S1324
S1325
先の各ハッシュ値
と各検証用ハッシュ値が一致
しない？
Yes
No
移動先保存装置にログイン処理する
S1326
全コンテンツデータを移動先原本保存装置に
移動モードで転送
S1327
全バージョン属性情報を移動先原本保存装置
に移動モードで転送
S1328
データ属性情報を移動先原本保存装置
に移動モードで転送
S1329
対象データの全コンテンツデータファイルを
削除
S1330
対象データの全バージョン属性情報ファイル
を削除
S1331
対象データのデータ属性情報ファイルを削除
S1332
移動したデータに対して保存データリスト
エントリ削除処理する
S1333
移動先保存装置からログアウト処理する
S1334
エンド
S1302
エラー処理

【図１８】



【図２９】

(a)

変更前	変更後
19990215　15：32：14　ID=1	19990215　15：30：00　ID=2
19990216　10：21：54　ID=2	19990116　10：22：00　ID=3
19990116　10：45：23　ID=3	19990216　10：46：00　ID=4

(b)

アクセス種別	アクセス日時	装置ＩＤ
CREATE	19990215　18：23：10　ID=1	R010-0001032
APPEND	19990215　18：23：30　ID=1	R010-0001032
MOVE TO	19990217　10：10：21　ID=3	R010-0001032
MOVE FROM	19990217　10：13：43　ID=2	R010-0001055

【図３２】

(a)

アカウントエントリ＃１	アカウント名
	パスワード
アカウントエントリ＃２	
アカウントエントリ＃３	
…	
アカウントエントリ＃Ｎ	

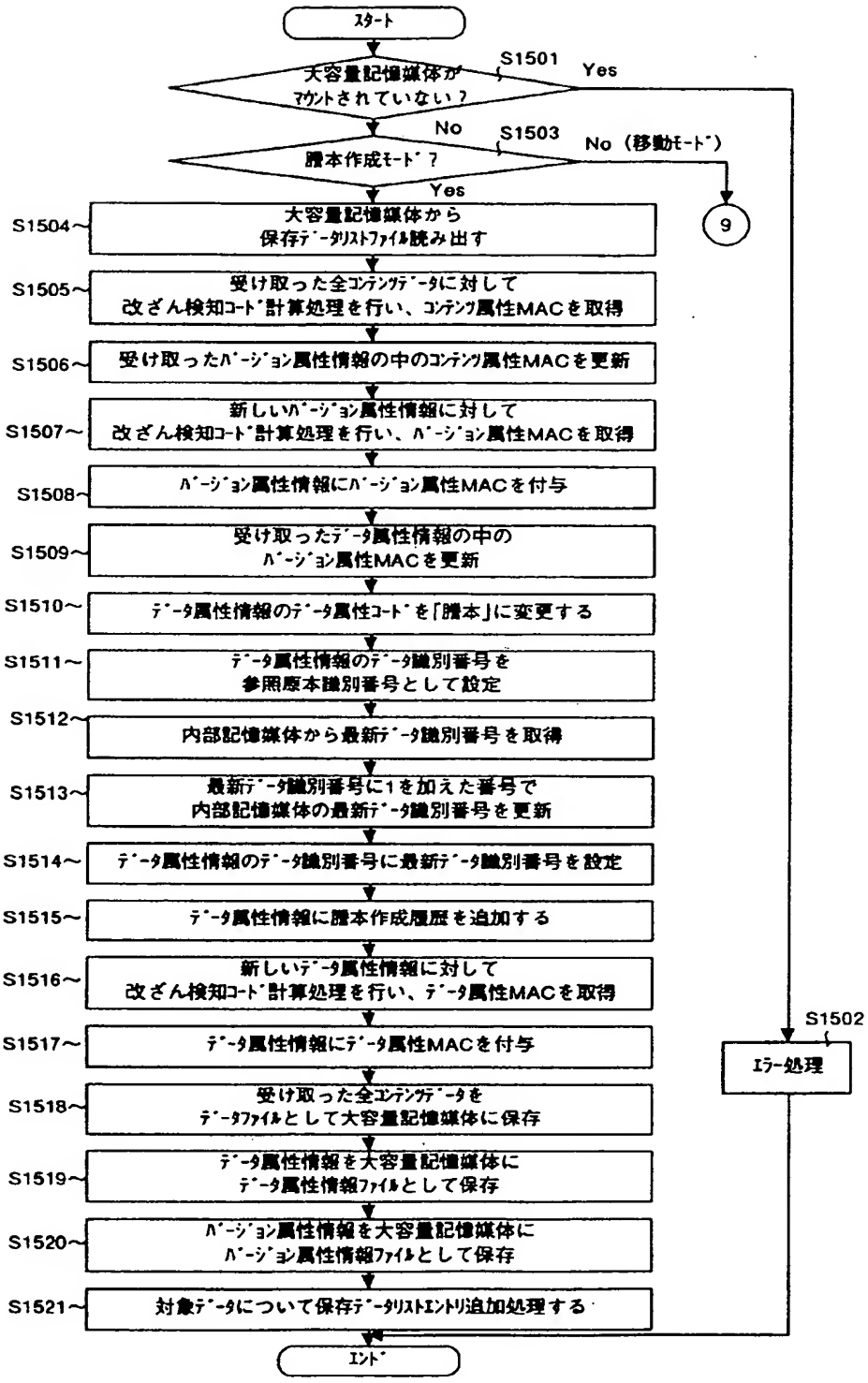
(b)

年
月
日
時
分
秒
GST（世界標準時）からのずれ
タイマID

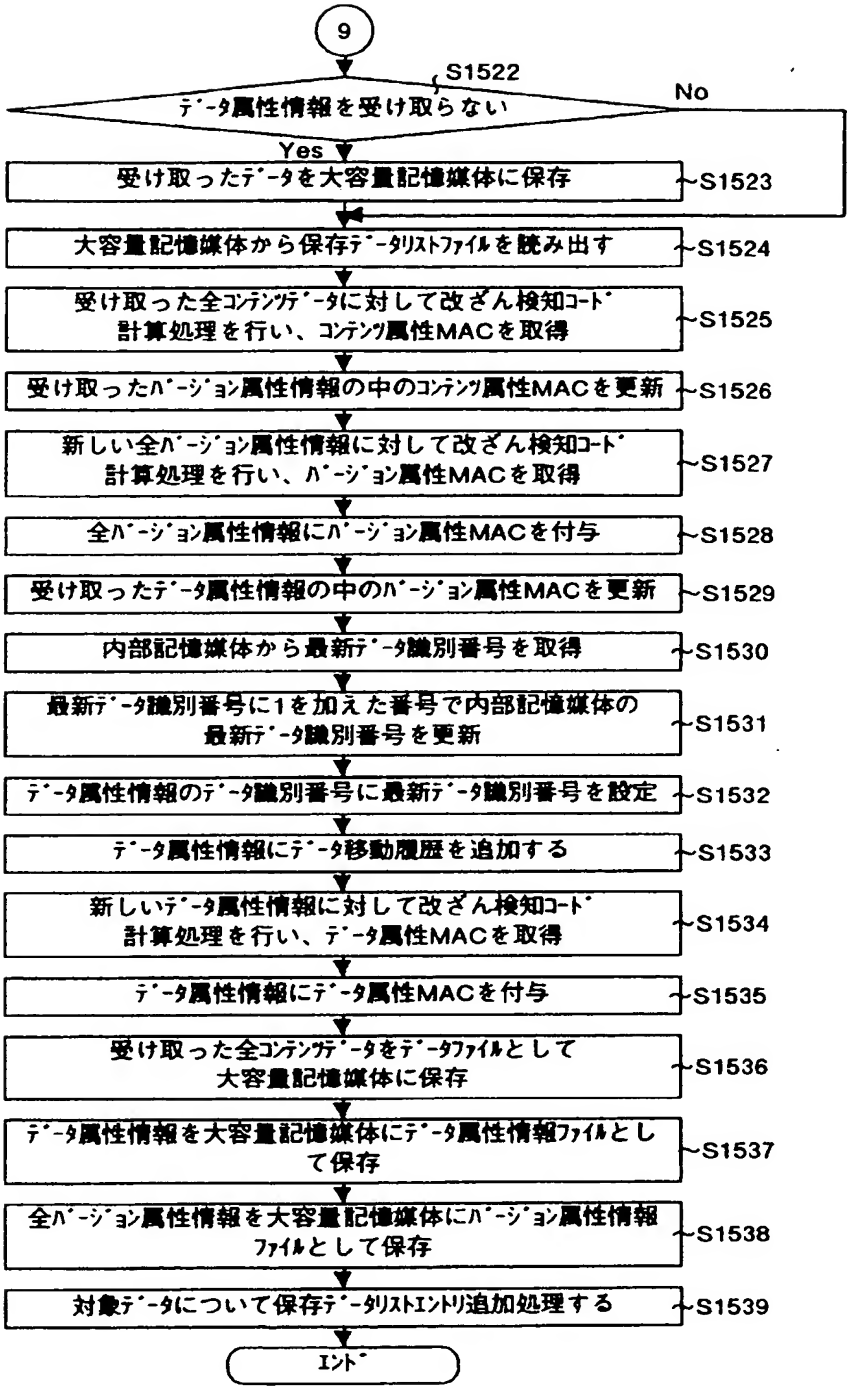
(c)

タイマ設定履歴＃１	設定前の日時情報
	設定後の日時情報
	アカウント名
タイマ設定履歴＃２	
タイマ設定履歴＃３	
…	
タイマ設定履歴＃Ｎ	

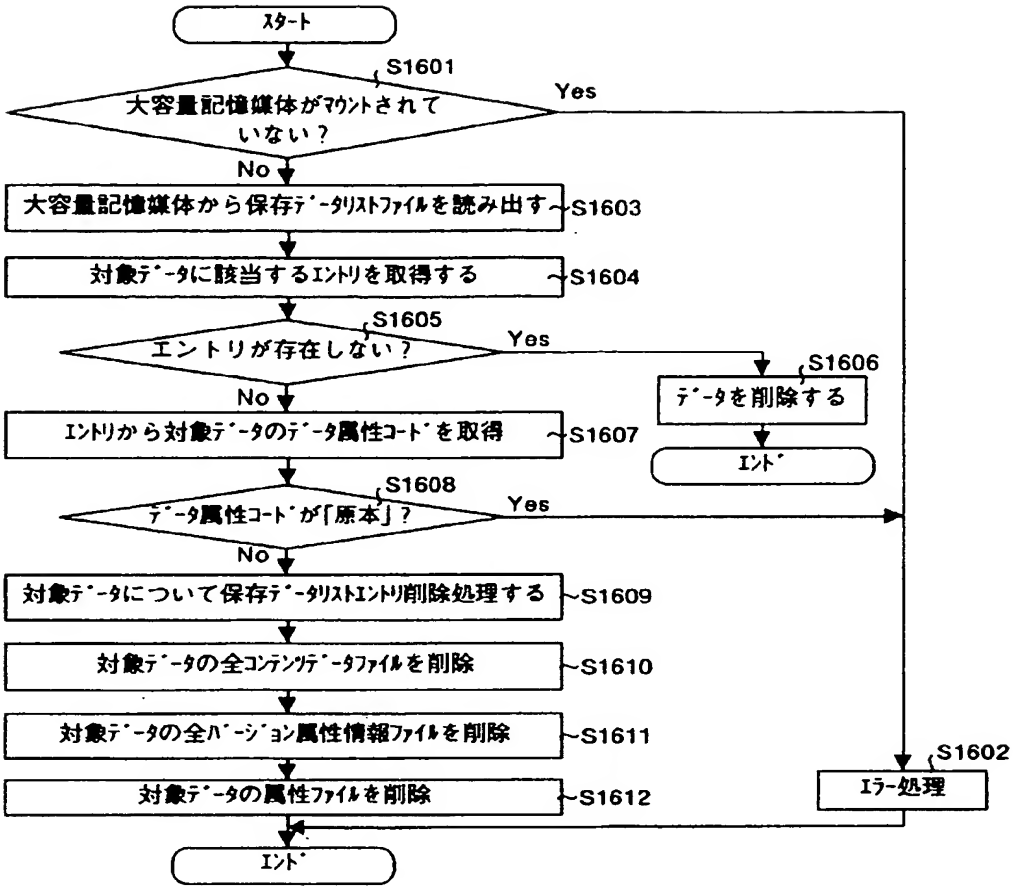
【図１９】


ｽﾀｰﾄ
S1501
大容量記憶媒体が
ﾏｳﾝﾄされていない？
Yes
No
S1503
謄本作成ﾓｰﾄﾞ？
No（移動ﾓｰﾄﾞ）
Yes
9
S1504
大容量記憶媒体から
保存ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙ読み出す
S1505
受け取った全ｺﾝﾃﾝﾂﾃﾞｰﾀに対して
改ざん検知ｺｰﾄﾞ計算処理を行い、ｺﾝﾃﾝﾂ属性MACを取得
S1506
受け取ったﾊﾞｰｼﾞｮﾝ属性情報の中のｺﾝﾃﾝﾂ属性MACを更新
S1507
新しいﾊﾞｰｼﾞｮﾝ属性情報に対して
改ざん検知ｺｰﾄﾞ計算処理を行い、ﾊﾞｰｼﾞｮﾝ属性MACを取得
S1508
ﾊﾞｰｼﾞｮﾝ属性情報にﾊﾞｰｼﾞｮﾝ属性MACを付与
S1509
受け取ったﾃﾞｰﾀ属性情報の中の
ﾊﾞｰｼﾞｮﾝ属性MACを更新
S1510
ﾃﾞｰﾀ属性情報のﾃﾞｰﾀ属性ｺｰﾄﾞを「謄本」に変更する
S1511
ﾃﾞｰﾀ属性情報のﾃﾞｰﾀ識別番号を
参照原本識別番号として設定
S1512
内部記憶媒体から最新ﾃﾞｰﾀ識別番号を取得
S1513
最新ﾃﾞｰﾀ識別番号に1を加えた番号で
内部記憶媒体の最新ﾃﾞｰﾀ識別番号を更新
S1514
ﾃﾞｰﾀ属性情報のﾃﾞｰﾀ識別番号に最新ﾃﾞｰﾀ識別番号を設定
S1515
ﾃﾞｰﾀ属性情報に謄本作成履歴を追加する
S1516
新しいﾃﾞｰﾀ属性情報に対して
改ざん検知ｺｰﾄﾞ計算処理を行い、ﾃﾞｰﾀ属性MACを取得
S1517
ﾃﾞｰﾀ属性情報にﾃﾞｰﾀ属性MACを付与
S1518
受け取った全ｺﾝﾃﾝﾂﾃﾞｰﾀを
ﾃﾞｰﾀﾌｧｲﾙとして大容量記憶媒体に保存
S1519
ﾃﾞｰﾀ属性情報を大容量記憶媒体に
ﾃﾞｰﾀ属性情報ﾌｧｲﾙとして保存
S1520
ﾊﾞｰｼﾞｮﾝ属性情報を大容量記憶媒体に
ﾊﾞｰｼﾞｮﾝ属性情報ﾌｧｲﾙとして保存
S1521
対象ﾃﾞｰﾀについて保存ﾃﾞｰﾀﾘｽﾄｴﾝﾄﾘ追加処理する
S1502
ｴﾗｰ処理
ｴﾝﾄﾞ

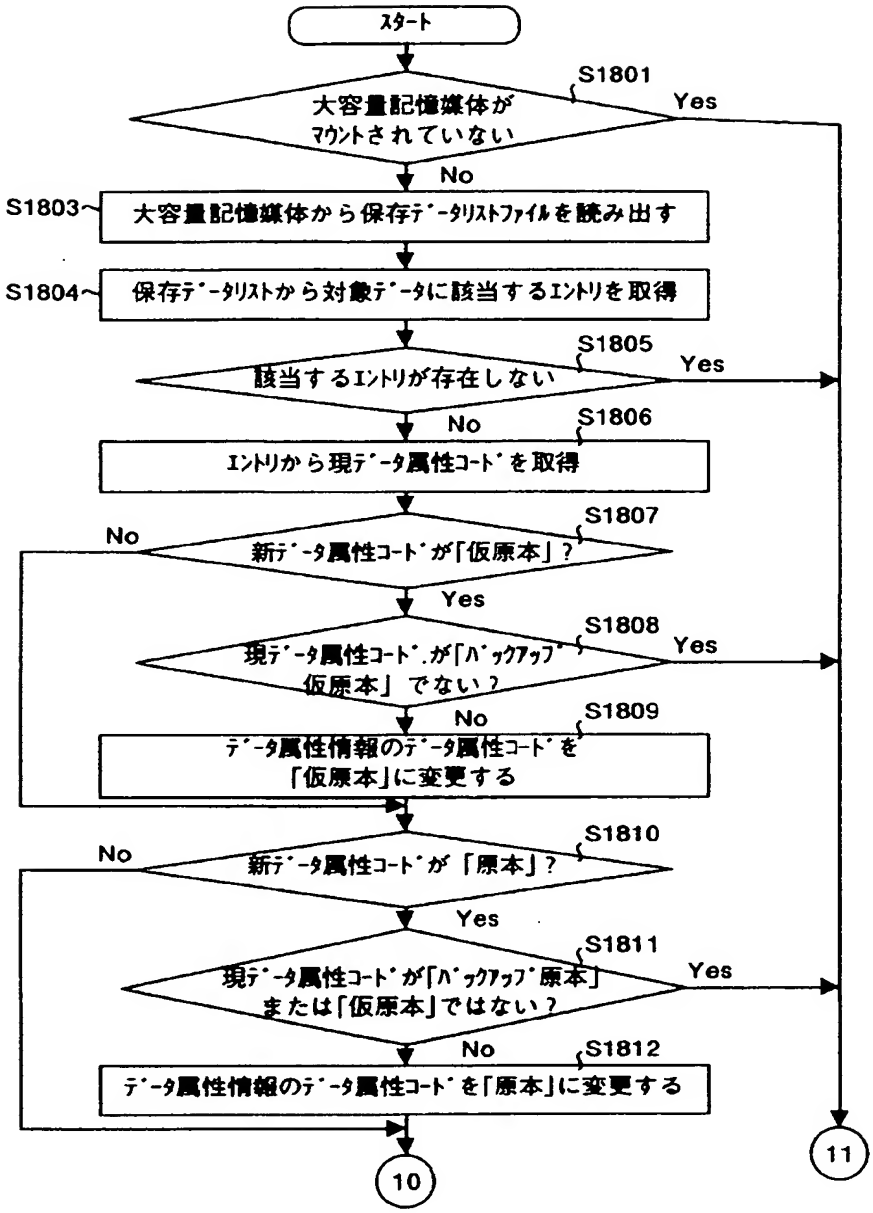
【図２０】


9
S1522
ﾃﾞｰﾀ属性情報を受け取らない
No
Yes
受け取ったﾃﾞｰﾀを大容量記憶媒体に保存
S1523
大容量記憶媒体から保存ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙを読み出す
S1524
受け取った全ｺﾝﾃﾝﾂﾃﾞｰﾀに対して改ざん検知ｺｰﾄﾞ計算処理を行い、ｺﾝﾃﾝﾂ属性MACを取得
S1525
受け取ったﾊﾞｰｼﾞｮﾝ属性情報の中のｺﾝﾃﾝﾂ属性MACを更新
S1526
新しい全ﾊﾞｰｼﾞｮﾝ属性情報に対して改ざん検知ｺｰﾄﾞ計算処理を行い、ﾊﾞｰｼﾞｮﾝ属性MACを取得
S1527
全ﾊﾞｰｼﾞｮﾝ属性情報にﾊﾞｰｼﾞｮﾝ属性MACを付与
S1528
受け取ったﾃﾞｰﾀ属性情報の中のﾊﾞｰｼﾞｮﾝ属性MACを更新
S1529
内部記憶媒体から最新ﾃﾞｰﾀ識別番号を取得
S1530
最新ﾃﾞｰﾀ識別番号に1を加えた番号で内部記憶媒体の最新ﾃﾞｰﾀ識別番号を更新
S1531
ﾃﾞｰﾀ属性情報のﾃﾞｰﾀ識別番号に最新ﾃﾞｰﾀ識別番号を設定
S1532
ﾃﾞｰﾀ属性情報にﾃﾞｰﾀ移動履歴を追加する
S1533
新しいﾃﾞｰﾀ属性情報に対して改ざん検知ｺｰﾄﾞ計算処理を行い、ﾃﾞｰﾀ属性MACを取得
S1534
ﾃﾞｰﾀ属性情報にﾃﾞｰﾀ属性MACを付与
S1535
受け取った全ｺﾝﾃﾝﾂﾃﾞｰﾀをﾃﾞｰﾀﾌｧｲﾙとして大容量記憶媒体に保存
S1536
ﾃﾞｰﾀ属性情報を大容量記憶媒体にﾃﾞｰﾀ属性情報ﾌｧｲﾙとして保存
S1537
全ﾊﾞｰｼﾞｮﾝ属性情報を大容量記憶媒体にﾊﾞｰｼﾞｮﾝ属性情報ﾌｧｲﾙとして保存
S1538
対象ﾃﾞｰﾀについて保存ﾃﾞｰﾀﾘｽﾄｴﾝﾄﾘ追加処理する
S1539
ｴﾝﾄﾞ

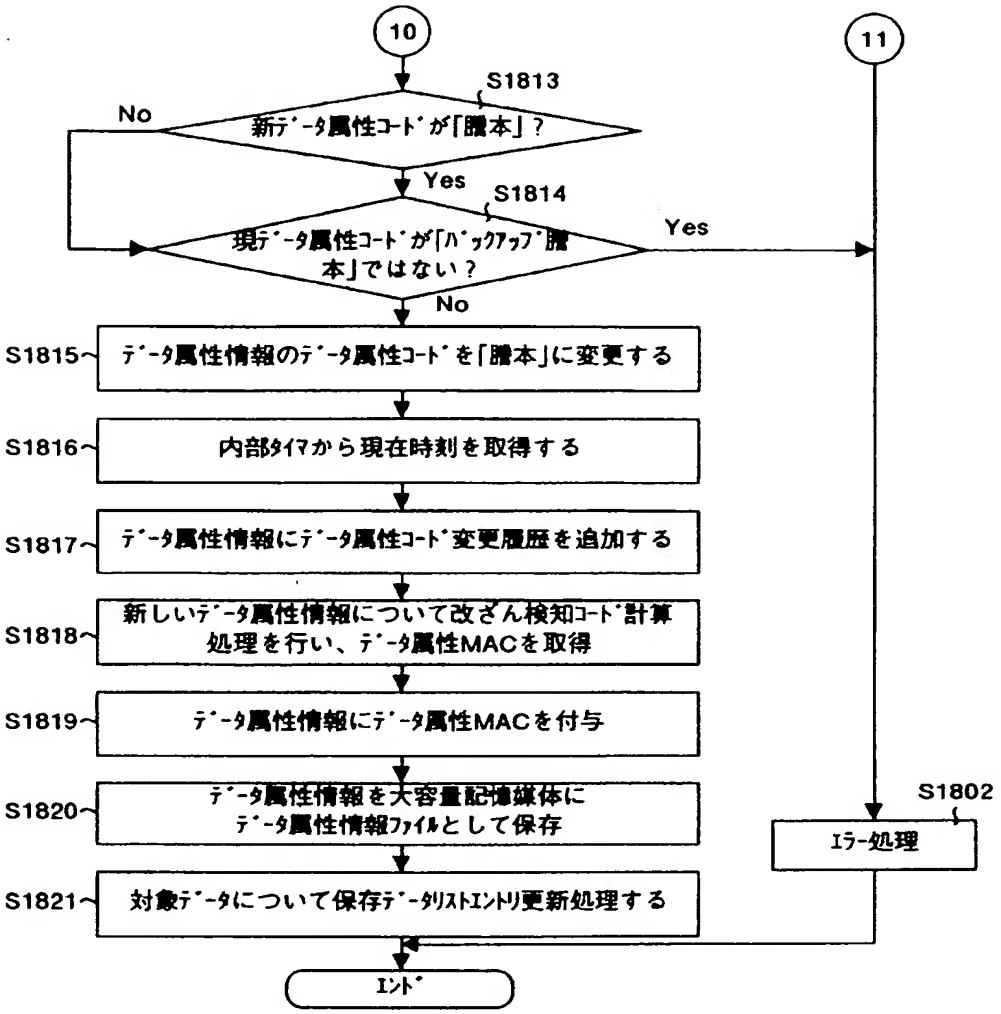
【図２１】


ｽﾀｰﾄ
S1601
大容量記憶媒体がﾏｳﾝﾄされていない？
Yes
No
大容量記憶媒体から保存ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙを読み出す
S1603
対象ﾃﾞｰﾀに該当するｴﾝﾄﾘを取得する
S1604
S1605
ｴﾝﾄﾘが存在しない？
Yes
S1606
ﾃﾞｰﾀを削除する
ｴﾝﾄﾞ
No
ｴﾝﾄﾘから対象ﾃﾞｰﾀのﾃﾞｰﾀ属性ｺｰﾄﾞを取得
S1607
S1608
ﾃﾞｰﾀ属性ｺｰﾄﾞが「原本」？
Yes
No
対象ﾃﾞｰﾀについて保存ﾃﾞｰﾀﾘｽﾄｴﾝﾄﾘ削除処理する
S1609
対象ﾃﾞｰﾀの全ｺﾝﾃﾝﾂﾃﾞｰﾀﾌｧｲﾙを削除
S1610
対象ﾃﾞｰﾀの全ﾊﾞｰｼﾞｮﾝ属性情報ﾌｧｲﾙを削除
S1611
対象ﾃﾞｰﾀの属性ﾌｧｲﾙを削除
S1612
S1602
ｴﾗｰ処理
ｴﾝﾄﾞ

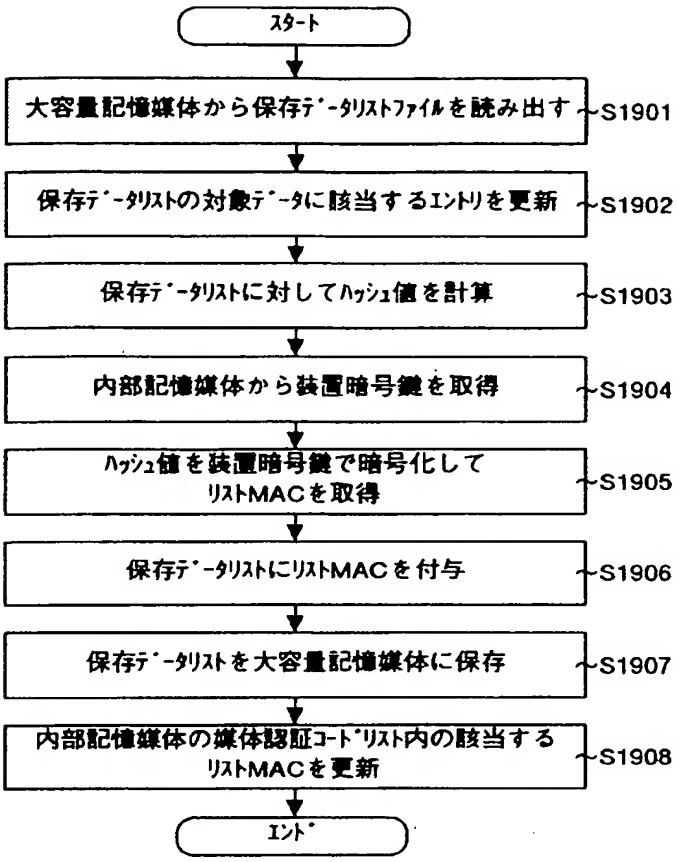
【図２３】


ｽﾀｰﾄ
S1801
大容量記憶媒体が
ﾏｳﾝﾄされていない
Yes
No
S1803
大容量記憶媒体から保存ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙを読み出す
S1804
保存ﾃﾞｰﾀﾘｽﾄから対象ﾃﾞｰﾀに該当するｴﾝﾄﾘを取得
S1805
該当するｴﾝﾄﾘが存在しない
Yes
No
S1806
ｴﾝﾄﾘから現ﾃﾞｰﾀ属性ｺｰﾄﾞを取得
S1807
No
新ﾃﾞｰﾀ属性ｺｰﾄﾞが「仮原本」？
Yes
S1808
現ﾃﾞｰﾀ属性ｺｰﾄﾞが「ﾊﾞｯｸｱｯﾌﾟ
仮原本」でない？
Yes
No
S1809
ﾃﾞｰﾀ属性情報のﾃﾞｰﾀ属性ｺｰﾄﾞを
「仮原本」に変更する
S1810
No
新ﾃﾞｰﾀ属性ｺｰﾄﾞが「原本」？
Yes
S1811
現ﾃﾞｰﾀ属性ｺｰﾄﾞが「ﾊﾞｯｸｱｯﾌﾟ原本」
または「仮原本」ではない？
Yes
No
S1812
ﾃﾞｰﾀ属性情報のﾃﾞｰﾀ属性ｺｰﾄﾞを「原本」に変更する
10
11

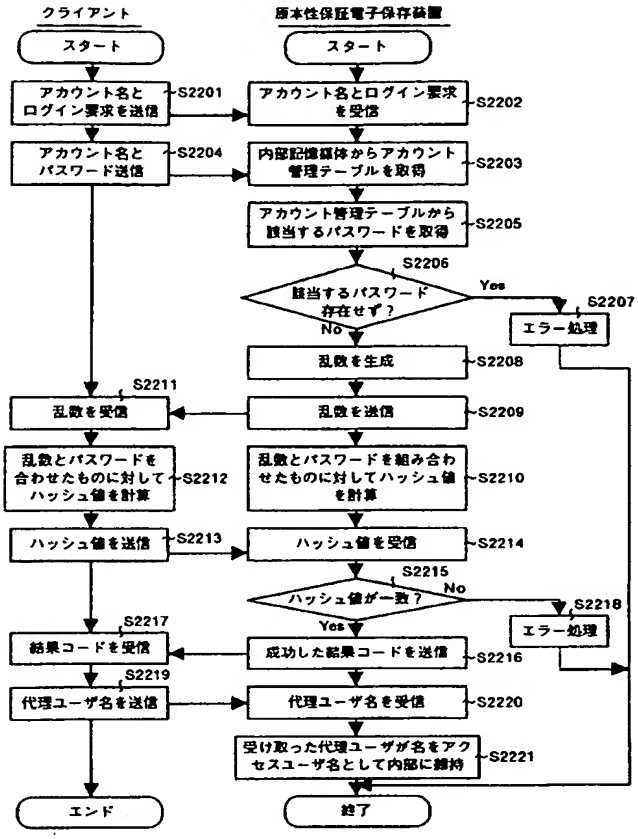
【図２４】


10
11
S1813
No
新ﾃﾞｰﾀ属性ｺｰﾄﾞが「謄本」？
Yes
S1814
現ﾃﾞｰﾀ属性ｺｰﾄﾞが「ﾊﾞｯｸｱｯﾌﾟ謄本」ではない？
Yes
No
S1815
ﾃﾞｰﾀ属性情報のﾃﾞｰﾀ属性ｺｰﾄﾞを「謄本」に変更する
S1816
内部ﾀｲﾏから現在時刻を取得する
S1817
ﾃﾞｰﾀ属性情報にﾃﾞｰﾀ属性ｺｰﾄﾞ変更履歴を追加する
S1818
新しいﾃﾞｰﾀ属性情報について改ざん検知ｺｰﾄﾞ計算処理を行い、ﾃﾞｰﾀ属性MACを取得
S1819
ﾃﾞｰﾀ属性情報にﾃﾞｰﾀ属性MACを付与
S1820
ﾃﾞｰﾀ属性情報を大容量記憶媒体にﾃﾞｰﾀ属性情報ﾌｧｲﾙとして保存
S1821
対象ﾃﾞｰﾀについて保存ﾃﾞｰﾀﾘｽﾄｴﾝﾄﾘ更新処理する
S1802
ｴﾗｰ処理
ｴﾝﾄﾞ

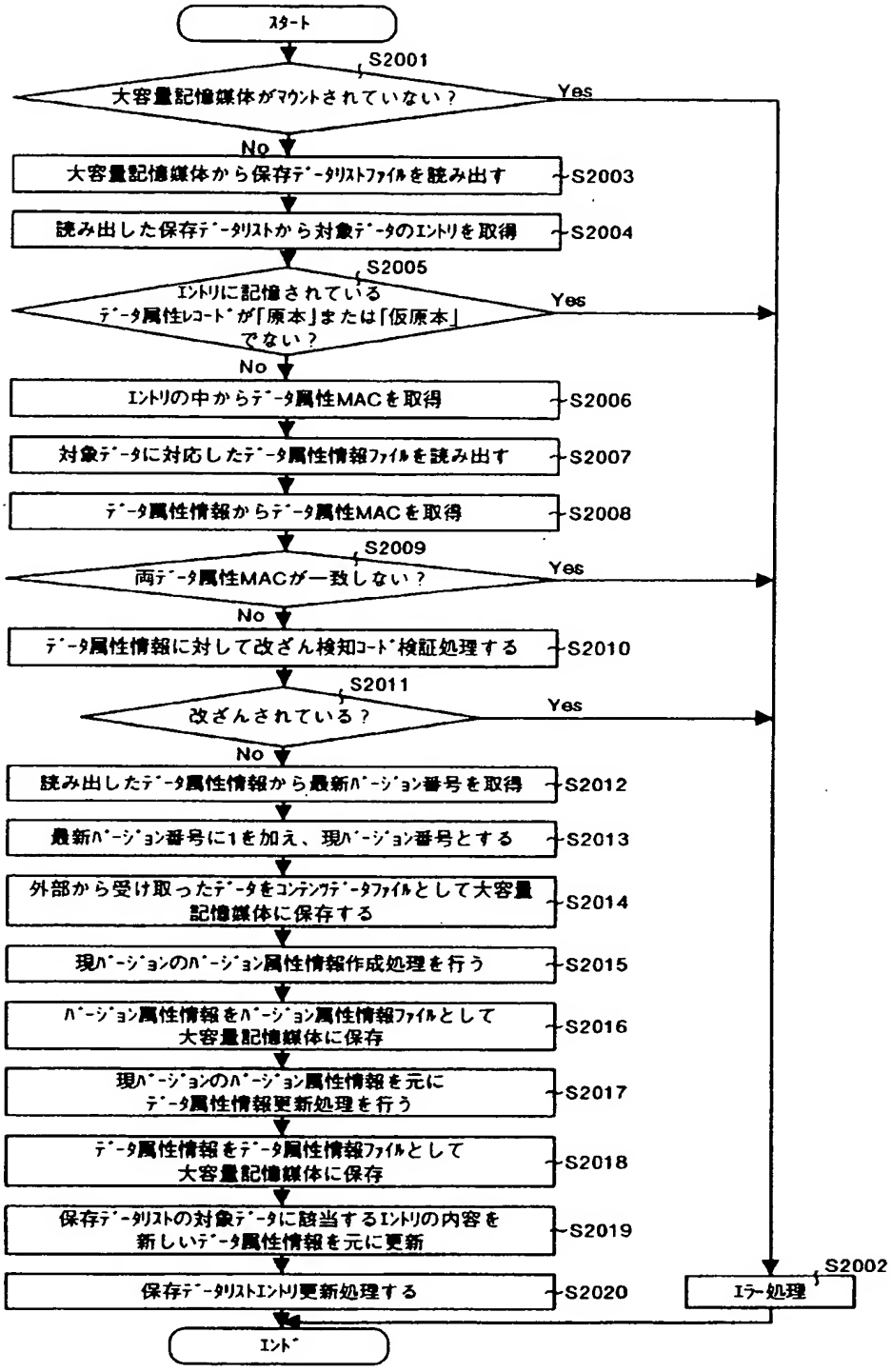
【図２５】


スタート
大容量記憶媒体から保存ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙを読み出す
S1901
保存ﾃﾞｰﾀﾘｽﾄの対象ﾃﾞｰﾀに該当するｴﾝﾄﾘを更新
S1902
保存ﾃﾞｰﾀﾘｽﾄに対してﾊｯｼｭ値を計算
S1903
内部記憶媒体から装置暗号鍵を取得
S1904
ﾊｯｼｭ値を装置暗号鍵で暗号化して
ﾘｽﾄMACを取得
S1905
保存ﾃﾞｰﾀﾘｽﾄにﾘｽﾄMACを付与
S1906
保存ﾃﾞｰﾀﾘｽﾄを大容量記憶媒体に保存
S1907
内部記憶媒体の媒体認証ｺｰﾄﾞﾘｽﾄ内の該当する
ﾘｽﾄMACを更新
S1908
ｴﾝﾄﾞ

【図２８】


クライアント
原本性保証電子保存装置
スタート
スタート
アカウント名とログイン要求を送信
S2201
アカウント名とログイン要求を受信
S2202
アカウント名とパスワード送信
S2204
内部記憶媒体からアカウント管理テーブルを取得
S2203
アカウント管理テーブルから該当するパスワードを取得
S2205
S2206
該当するパスワード存在せず？
Yes
S2207
エラー処理
No
乱数を生成
S2208
S2211
乱数を受信
乱数を送信
S2209
乱数とパスワードを合わせたものに対してハッシュ値を計算
S2212
乱数とパスワードを組み合わせたものに対してハッシュ値を計算
S2210
ハッシュ値を送信
S2213
ハッシュ値を受信
S2214
S2215
ハッシュ値が一致？
No
S2218
エラー処理
Yes
S2217
結果コードを受信
成功した結果コードを送信
S2216
S2219
代理ユーザ名を送信
代理ユーザ名を受信
S2220
受け取った代理ユーザが名をアクセスユーザ名として内部に維持
S2221
エンド
終了

【図２６】


ｽﾀｰﾄ
S2001
大容量記憶媒体がﾏｳﾝﾄされていない？
Yes
No
大容量記憶媒体から保存ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙを読み出す
S2003
読み出した保存ﾃﾞｰﾀﾘｽﾄから対象ﾃﾞｰﾀのｴﾝﾄﾘを取得
S2004
S2005
ｴﾝﾄﾘに記憶されている
ﾃﾞｰﾀ属性ﾚｺｰﾄﾞが「原本」または「仮原本」
でない？
Yes
No
ｴﾝﾄﾘの中からﾃﾞｰﾀ属性MACを取得
S2006
対象ﾃﾞｰﾀに対応したﾃﾞｰﾀ属性情報ﾌｧｲﾙを読み出す
S2007
ﾃﾞｰﾀ属性情報からﾃﾞｰﾀ属性MACを取得
S2008
S2009
両ﾃﾞｰﾀ属性MACが一致しない？
Yes
No
ﾃﾞｰﾀ属性情報に対して改ざん検知ｺｰﾄﾞ検証処理する
S2010
S2011
改ざんされている？
Yes
No
読み出したﾃﾞｰﾀ属性情報から最新ﾊﾞｰｼﾞｮﾝ番号を取得
S2012
最新ﾊﾞｰｼﾞｮﾝ番号に1を加え、現ﾊﾞｰｼﾞｮﾝ番号とする
S2013
外部から受け取ったﾃﾞｰﾀをｺﾝﾃﾝﾂﾃﾞｰﾀﾌｧｲﾙとして大容量
記憶媒体に保存する
S2014
現ﾊﾞｰｼﾞｮﾝのﾊﾞｰｼﾞｮﾝ属性情報作成処理を行う
S2015
ﾊﾞｰｼﾞｮﾝ属性情報をﾊﾞｰｼﾞｮﾝ属性情報ﾌｧｲﾙとして
大容量記憶媒体に保存
S2016
現ﾊﾞｰｼﾞｮﾝのﾊﾞｰｼﾞｮﾝ属性情報を元に
ﾃﾞｰﾀ属性情報更新処理を行う
S2017
ﾃﾞｰﾀ属性情報をﾃﾞｰﾀ属性情報ﾌｧｲﾙとして
大容量記憶媒体に保存
S2018
保存ﾃﾞｰﾀﾘｽﾄの対象ﾃﾞｰﾀに該当するｴﾝﾄﾘの内容を
新しいﾃﾞｰﾀ属性情報を元に更新
S2019
保存ﾃﾞｰﾀﾘｽﾄｴﾝﾄﾘ更新処理する
S2020
S2002
ｴﾗｰ処理
ｴﾝﾄﾞ

フロントページの続き

(51) Int.Cl.[7]	識別記号	FI	テーマコード(参考)
		G06F 15/401	340B

Fターム(参考) 5B017 AA02 BA02 BB06 CA16
5B049 CC00 EE05 GG02 GG10
5B075 KK54 NR20 NS10 QS01 UU06
5B082 AA00 DD08 EA01 EA07 EA11
GA05 GA11 GA20